UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

	)
Notice of proposed rulemaking	)
Cyber Security Incident Reporting	) Docket Nos. RM18-2-000
Reliability Standards	) and AD17-9-000
(Issued December 21, 2017)	)

Comments of Mark S. Simon
In Response to Notice of Proposed Rulemaking

1. I am an individual submitting these comments in response to the Commission's Notice of Proposed Rulemaking for Cyber Security Incident Reporting Reliability Standards ("NOPR").[1]

2. I am a U.S. citizen and my place of business is located at 1340 N. Astor, Chicago, Illinois. I own Simon Cyber Group, LLC, a consulting firm engaged in providing systems security and compliance consulting services to the electricity sector. I hold the Certified Information Systems Security Professional (CISSP) certification from ISC^2 and the Global Industrial Cyber Security Professional (GICSP) from GIAC. I have been engaged in NERC CIP security and compliance consulting services since 2008.

3. I write to encourage the Federal Energy Regulatory Commission ("Commission") to broaden its directive to NERC to include specific reporting requirements pertaining to malicious disruptions or attempts to compromise electronic access controls for BES assets with low impact BES Cyber Systems.

4. The Federal Energy Regulatory Commission ("Commission") suggests at par. 3 of the NOPR that a gap exists in the current reporting threshold for Cyber Security Incidents.[2]

[1] *Cyber Security Incident Reporting Reliability Standards*, Notice of Proposed Rulemaking, 82 Fed. Reg. 61499 (December 28, 2017), 161 FERC ¶ 61,291 (2017).

[2] *Id.*, par. 3.

5. While I agree the reporting gap exists, I believe the reporting gap potentially applies to electronic access controls associated with all types of BES Cyber Systems, whether classified as high, medium or low.

6. The Commission's proposed directive to NERC to address the reporting gap sufficiently closes the reporting gap for electronic access controls associated with high and medium impact BES Cyber Systems but falls short with respect to electronic access controls for low impact BES Cyber Systems. The Commission proposes to direct NERC "to develop modifications to the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)."[3] Since these terms are used throughout the CIP Reliability Standards in the context of requirements applicable only to high and medium impact BES Cyber Systems, the Commission's directive does not stretch far enough to encompass reporting requirements applicable to similar electronic access controls for BES assets with low impact BES Cyber Systems.

7. Currently, mandatory reporting of a Cyber Security Incident involving a BES asset with a low impact BES Cyber System is addressed in CIP-003-6, Requirement 2, Attachment 1, Section 4.2:

> Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:
>
> 4.1 Identification, classification, and response to Cyber Security Incidents;
>
> 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;
>
> …

[3] *Id.*, par.4.

Application of the definition of a "Cyber Security Incident" would be a preliminary step in determining whether the classification of a "Reportable Cyber Security Incident" applies to an incident involving an electronic access control for a BES asset with a low impact BES Cyber System.[4]

8. The NERC Glossary definition of a "Cyber Security Incident" is:

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.

9. Since "Electronic Security Perimeter" is associated in the CIP Reliability Standards solely with high and medium impact BES Cyber Systems, the definition of a Cyber Security Incident does not necessarily encompass an electronic access control, such as a domain controller or router, that controls electronic access to a low impact BES Cyber System.

10. Moreover, the reporting gap is not closed in the proposed CIP-003-7 Reliability Standard.[5] Neither "Electronic Security Perimeter" nor "Electronic Access Control or Monitoring Systems" are terms applied to electronic access controls for low impact BES Cyber Systems in the proposed CIP-003-7 Reliability Standard. Rather, the Guidelines and Technical Basis Section of CIP-003-7 describes applicable electronic

[4] The meaning of "Cyber Security Incident" and "Reportable Cyber Security Incident" are set forth in the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary"), available at http://www.nerc.com/files/Glossary_of_Terms.pdf.

[5] On October 19, 2017, the Commission issued a notice of proposed rulemaking proposing to approve proposed Reliability Standard CIP-003-7. See Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls, Notice of Proposed Rulemaking, 82 Fed. Reg. 49,541 (October 26, 2017), 161 FERC ¶ 61,047 (2017). The modifications in proposed Reliability Standard CIP-003-7 improve upon the existing protections applicable to low impact BES Cyber Systems, consistent with the Commission's directives in FERC Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, 81 Fed. Reg. 4177 (2016) by, in part, clarifying the electronic access control requirements applicable to low impact BES Cyber Systems.

security controls as those that can be drawn from "a flexible selection … that can meet operational needs as well as the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset."[6]

11. Omission of mandatory reporting for the disruption, or an attempt to disrupt, the operation of electronic 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, and the Commission's desire to improve awareness of existing and future cyber security threats and potential vulnerabilities.

12. At par. 7 of the NOPR on Cyber Security Incident Reporting Reliability Standards, the Commission cites the contention of Resilient Societies that "[A]n infected low impact BES Cyber System can serve as an entry point from where an adversary can attack medium and high impact BES Cyber Systems.[7]

13. Resilient Societies further asserts in its Petition that a "simultaneous cyberattack on many low impact assets may cause greater impact than an attack on a single high impact asset."[8]

14. The threats and potential impacts identified by the Resilient Societies warrants further action by the Commission in closing the reporting gap for incidents affecting electronic access controls applicable to BES assets with low impact BES Cyber Systems.

[6] CIP-003-7, Guidelines and Technical Basis Section, page 33 of 57.

[7] *Cyber Security Incident Reporting Reliability Standards*, Notice of Proposed Rulemaking, 82 Fed. Reg. 61499 (December 28, 2017), 161 FERC ¶ 61,291 (2017), at par. 7.

[8] Resilient Societies Petition at 2-3. Resilient Societies' filings and responsive comments are available on the Commission's eLibrary document retrieval system in Docket No. AD17-9-000.

15. In conclusion, I respectfully request that the Commission consider these comments and broaden the Commission's directive to NERC to include mandatory reporting of incidents involving electronic access controls for low impact BES Cyber Systems.

Respectfully submitted,

/s/ Mark S. Simon

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting Reliability Standards	))))	Docket No. RM18-2-000 AD17-9-000

COMMENTS OF THE NEW YORK STATE
PUBLIC SERVICE COMMISSION

INTRODUCTION

On December 28, 2017, the Federal Energy Regulatory Commission (FERC or the Commission) published a Notice of Proposed Rulemaking (NOPR) in the Federal Register seeking comments on a Commission proposal to direct the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Reliability Standards to improve mandatory reporting of Cyber Security Incidents.[1] Currently, breaches of cyber security "must be reported only if they have 'compromised or disrupted one or more reliability tasks.'"[2] With this NOPR, the Commission proposes to require reporting of incidents before they cause harm, or even if the incident did

[1] Docket Nos. RM18-2-000 and AD17-9-000, Cyber Security Incident Reporting Reliability Standards, 161 FERC ¶61,291 (issued December 21, 2017) (NOPR).

[2] Id. at 1.

not cause any harm.[3] The intent is to "enhance awareness for NERC, industry, the Commission, other federal and state entities, and interested stakeholders regarding existing or developing cyber security threats."[4]

The New York State Public Service Commission (NYPSC) applauds the Commission for its interest and efforts in strengthening cyber security reporting standards.[5] However, the proposed mandatory reporting requirements do not include any obligations to notify appropriate state entities[6] when an incident occurs. The NYPSC therefore respectfully urges the Commission to direct NERC to share incident reports with appropriate state entities charged with responsibility for critical infrastructure protection, so the state entities may respond timely, appropriately, and take defensive measures in concert with their federal partners.

BACKGROUND

Under the Federal Power Act, NERC, as the Commission's certified Electric Reliability Organization (ERO), is authorized

[3] Id.

[4] Id. at 3.

[5] The views expressed herein are not intended to represent those of any individual member of the NYPSC. Pursuant to Section 12 of the New York Public Service Law, the Chair of the NYPSC is authorized to direct this filing on behalf of the NYPSC.

[6] Appropriate State entities should be those charged with responsibility for critical infrastructure protection. This will differ from state-to-state.

to create Reliability Standards, subject to Commission review and approval.[7] Pursuant to its authority, NERC authored requirements for cyber security incident reporting.[8] NERC's current standards define a reportable cyber security incident as one "that has compromised or disrupted one or more reliability tasks of a functional entity."[9] This definition, however, essentially necessitates a cyber security attack to breach protections and cause some form of disruption to be reported. The Commission notes that while these Cyber Security Standards were in place, extremely few incidents were reported from 2014 – 2016,[10] yet the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 79 cyber security incidents in 2014 and 46 in 2015.[11]

On January 13, 2017, Resilient Societies filed a Petition requesting that the Commission "initiate a rulemaking to require an enhanced Reliability Standard for malware detection, reporting, mitigation and removal from the Bulk-Power

[7] Federal Power Act §215, 16 U.S.C. §824o(e).

[8] Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning).

[9] Id. at Requirement R1 at p. 26.

[10] Docket Nos. RM18-2-000, AD17-9-000, NOPR at 7, citing, Docket No. AD17-9-000, Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System, Foundation for Resilient Societies Petition for Rulemaking (Jan.13, 2017) at 8-9 (Resilient Societies' Petition).

[11] Id.

System."[12] Resilient Societies identified a number of vulnerabilities that cyber hackers can use to take advantage of the bulk power system, and explained that these vulnerabilities, if breached, "can result in instability, uncontrolled separation, and cascading failures."[13] Within its Petition, Resilient Societies illustrates that the reporting of cybersecurity incidents is relatively low compared to the number of incidents that occur. Based on the Resilient Societies' Petition, the Commission issued the NOPR.[14]

DISCUSSION

The NYPSC supports FERC's ongoing efforts to strengthen cybersecurity of the bulk power system. Security is an ever-changing environment; federal and state regulators and the industry must continue to adapt to thwart new possible attacks. New York State is as committed to this goal as FERC.

However, if the Commission adopts the proposal as it is presently comprised, the only additional information that state entities would gain is an annual compilation of incidents

[12] Id. at 4, citing, Resilient Societies' Petition.

[13] Resilient Societies' Petition at 3.

[14] Within its Petition, Resilient Societies requested that the Commission also require additional measures for malware detection, mitigation, and removal, in addition to improved rules for reporting. The Commission decided not to propose additional Reliability Standards for malware detection, mitigation, and removal at this time based on other ongoing efforts to improve Reliability Standards. NOPR at 1.

reported to federal entities. This proposed change may amount to a little information received too late. An annual report would fail to provide states with sufficient information on a timely basis so that they can ensure that corrective actions can be taken, as warranted. An unsuccessful cyber attack identified by a utility might not be made known to appropriate state entities for as much as twelve months after the event.

To truly help states jointly assist in the defense of cyber attacks, and further the objectives of the NOPR, appropriate state entities[15] should also be provided with the same information when it is filed with the federal authorities. This would allow appropriate state entities to obtain critical information of cyber attacks when the incident occurs, and would assist FERC in achieving its stated goal of enhancing awareness for NERC, the industry, the Commission, other federal and state entities, and interested stakeholders.[16]

However, NYPSC also understands that some NERC entities are concerned that the NOPR may generate voluminous reports of cyber incidents. Failed cyber attacks occur on a continuous basis, all the time. A reporting requirement of

[15] For New York State, the appropriate state entities would include the New York State Department of Public Service, and New York State Division of Homeland Security & Emergency Services.

[16] NOPR at 3.

every attempted security attack may be overly burdensome for reporting entities. Additionally, numerous reports of every attempted routine cyber attack may provide little beneficial data in a plethora of reports. NYPSC suggests FERC consider developing clear criteria of the required reporting based on its review of the comments and recommendations from reporting entities.

CONCLUSION

For the reasons set forth herein, the NYPSC respectfully urges the Commission to modify the proposed reporting requirements of the Reliability Standard to include the reporting of incidents to appropriate state entities, and to approve the amended proposal.

Respectfully submitted,

s/ Paul Agresta

Paul Agresta
General Counsel
Public Service Commission
of the State of New York
By: Alan T. Michaels
Manager
3 Empire State Plaza
Albany, New York 12223-1350
Tel: (518) 474-1585
Alan.Michaels@dps.ny.gov

Dated: February 16, 2018
Albany, New York

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Notice of Proposed Rulemaking	**)**	
Cyber Security Incident Reporting	**)**	**Docket No. RM18-2-000**
Reliability Standards	**)**	**and AD17-9-000**

COMMENTS OF NRG ENERGY, INC.

NRG Energy, Inc. ("NRG") submits the following comments to the Federal Energy Regulatory Commission ("FERC" or "Commission") in response to the December 21, 2017 Notice of Proposed Rulemaking (NOPR).[1] Through its subsidiaries, NRG owns one of the largest power generation fleets in the United States. NRG engages in wholesale power generation, retail electric supply, and deployment and commercialization of alternative technologies, and therefore, has a strong interest in the proposed rulemaking. NRG supports many aspects of the NOPR as more fully discussed below.

I. BACKGROUND

The Commission issued the NOPR proposing to direct NERC to modify its CIP Reliability Standards to broaden the mandatory reporting requirements for cyber security incidents. Specifically, the Commission seeks comment on developing and submitting modifications to the NERC Reliability Standards to improve mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system.

[1] *Notice of Proposed Rulemaking Cyber Security Incident Reporting Reliability Standards*, Docket No. RM18-2-000 and AD17-9-00 (issued December 21, 2017) ("NOPR").

II. COMMENTS

NRG supports direction to NERC to develop modifications to the CIP Reliability Standards to improve the reporting of Cyber Security Incidents[2]. Specifically, NRG provides the below comments.

The Commission states that "[s]ince an ESP is intended to protect BES Cyber Systems and EACMS are intended to control electronic access into an ESP, we believe it is reasonable to establish the compromise of, or attempt to compromise, an ESP or its associated EACMS as the minimum reporting threshold."[3] However, this 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 Systems. Therefore, in order to improve the reporting of Cyber Security Incidents (which NRG fully supports), NRG believes any modifications to the referenced CIP Reliability Standards should be applicable to all BES Cyber Systems with External Routable Communications.

FERC also states that "In sum, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop modifications to the CIP Reliability Standards described above to improve the reporting of Cyber Security Incidents, including incidents that did not cause any harm but could facilitate subsequent efforts to harm the reliable operation of the bulk electric system."[4] NRG concurs with the Commission's proposed rulemaking for modifications of the CIP Reliability Standards with focus on the inclusion of attempts and/or incidents that did not cause any harm but could facilitate subsequent efforts to harm, the reliable

[2] NOPR at P 35.

[3] NOPR at P 34.

[4] NOPR at P 35.

operation of the bulk electric system. However, NRG specifically recommends that requirement language modifications should include [only] *attempts to disrupt or compromise access of control systems (minimal risk incidents relating to access of control systems, rather than those minimal risk incidents involving all systems of an entire company).* Therefore, NRG requests the Commission consider expanding the standard scope to include modification or development of NERC (CIP) terminology relating to attempt and incident reporting relating to those personnel that have BES Cyber System access as well as BES Cyber Systems with control capability.

NRG recommends that the modifications provide clear guidance on requirement expectations for initial/preliminary reporting detail required when complete investigations of an incident are underway by an entity. In the context of modifications to the CIP standards, the NERC glossary term "Reportable Cyber Security Incident" may need modification or technical clarification / guidance from NERC so that industry participants can clearly identify an attack versus noise in the system or specify evaluation of directed events versus non-directed events.

In addition, NRG recommends that the term "attempt" become clear criteria within the context of modifications to the CIP standard for this NOPR [for example, an "attempt" should be clarified as a more serious risk than a port scan] and should be provided in technical guidance or glossary definition relating to the context of existing NERC glossary term: "Cyber Security Incident". NRG also recommends that the modifications to CIP standards include the US-CERT defined terminology of "attack".[5] NRG recommends that the Commission direct NERC to provide technical guidance or glossary definition relating to the context of existing NERC

[5] "Attack" is defined as an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. Extended Definition: The intentional act of attempting to bypass one or more security services or controls of an information system. See https://niccs.us-cert.gov/glossary.

glossary term: Reportable Cyber Security Incident (or Cyber Security Incident) as it relates to these additionally referenced terms.

In terms of gathering information related to these events, NRG recommends that the Commission consider directing NERC to participate with the E-ISAC to develop or utilize an automated data management system with specific field entry and examples to ease industry and user reporting of initial event details while incident investigation is occurring.

As requested in paragraph 36 of the NOPR, the Commission seeks "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. . . ." NRG does not assert that a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure would effectively address the reporting gap. Moreover, the request for data or information would also neither address current lack of awareness of cyber-related incidents discussed above, nor satisfy the goals of the proposed directive. NRG instead recommends requiring that organizations implement a process to assess "attempts", while not requiring reporting the attempts as part of "Reportable Cyber Security Incidents". This would improve industry awareness of potential cyber-attacks while maintaining an organization's ability to appropriately respond to actual Cyber Security Incidents of a reportable threshold. [For example, if the event is an attempt at compromise, the organization *should* report it (either without a time requirement or within a time requirement significantly longer than a 24 hour reporting threshold)]. NERC could address this by adding a new requirement to CIP-008 instead of creating a separate or new CIP standard. Active participation in this process, could serve as a demonstration of a registered entity's assessment and management of risk as part of its security program and active participation in reporting and assessment with the Industry. In doing so, the registered entity may inherently pose less of a risk to the BES (as could be evaluated in an entity's Inherent Risk Assessment with the regional entities).

In paragraph 35 of the NOPR, the Commission seeks "comment regarding inclusion of EACMS in the scope of the NOPR. . . ." As noted above, NRG asserts no objection to the inclusion of EACMS in the scope of this NOPR and recommends that the scope of the NOPR avoid limiting the requirement to High and Medium Impact BES Cyber Systems.

Regarding the Commission's request in paragraph 40 for comments on the appropriate content for Cyber Security Incident reporting, NRG recommends that required reporting as part of the additional scope include: content Date, Time, Duration of Incident, Origination of the attack, threat vector, targeted system (or OS), vulnerability exploited, & method used to stop / prevent the attack. This would provide for effective lessons learned and awareness for the industry. Also, as noted above, NRG also recommends that the modifications provide clear guidance on requirement expectations for initial/preliminary reporting detail required when complete investigations of an incident are underway by an entity. In the context of modifications to the CIP standards for these reasons, the NERC glossary term "Reportable Cyber Security Incident" may need modification or technical clarification / guidance from NERC so that the industry participants can clearly identify an attack versus noise in the system or specify evaluation of directed events versus non-directed events.

In regards to the appropriate timing for Cyber Security Incident reporting,[6] NRG recommends that the appropriate timing for *Cyber Security Incident reporting relating to modifications for and/or incidents that did not cause any harm but could facilitate subsequent efforts to harm the reliable operation of the bulk electric system* be required to occur after

[6] NOPR P 43.

existing industry processes have been followed relating to Incident Reporting and Response Plans. In addition, NRG recommends that a potential incident identified as an "attempt" into this category, be defined as not Reportable, and instead be considered to be optionally Reportable through less stringent or non-required timeframes for reporting (and that the scope of NERC requirements for this information be managed under the existing CIP standards) so that the information of the attempt or incident is not treated as a Reportable Cyber Security Incident, per the existing NERC glossary of terms. Moreover, NRG recommends that entities have a requirement to implement a process to assess the scope of "attempts" and that those registered entities that participate in reporting receive credit for their efforts through Regional Entities during the Inherent Risk Assessment process. NRG asserts that this additional scope of requirements could be addressed by updating the requirements under CIP-008 rather than by creating a new CIP standard.

Lastly, NRG recommends that the Commission consider directing NERC to file a quarterly report in addition to the annual report outlined in paragraph 42 of the NOPR. The annual report assists companies in setting a security strategy while a quarterly report assists companies in configuring existing security architecture.

IV. CONCLUSION

For the aforementioned reasons, NRG broadly supports the NOPR and appreciates consideration of the enclosed comments.

February 19, 2018

Respectfully submitted,

/s/ Kara White
Kara White
Director, Regulatory Compliance
NRG Energy, Inc.
804 Carnegie Center
Princeton, NJ 08540

Document Content(s)

File FERC Rulemaking.DOCX cannot be converted to PDF.

Document Content(s)

Docket Number RM18-2-000

My name is Dr. Fred A. Reitman. I am a U.S. citizen residing in Houston, Texas. I am writing in support of the Foundation for Resilient Societies Jan. 13, 2017 petition requesting that FERC make NERC accountable for robust cyber security standards. I do not believe current regulations are adequate to protect the U.S. electric grid.

My professional background is in toxicology; specifically I hold a Ph.D in Environmental Health and am a Diplomate of the American Board of Toxicology. I am now a retired private citizen. I have no vested interest in this rule-making other than as a concerned citizen. Specifically I am not employed by FERC, NERC, or any private company involved with generation, transmission or distribution of electric power.

I believe the U.S. electric grid vulnerability poses a very real and existential threat to our country. Currently the grid can be intentionally attacked and shut down at any time by cyber, physical or EMP attack, or by a severe solar flare strike. The Congressional EMP Commission estimated that 90% or more Americans would perish should a prolonged, widespread grid shut-down occur.

A robust regulatory oversight process is clearly needed in light of this threat. But that is not what we currently have. Instead, the current regulatory process amounts to a 'fox guarding the henhouse' process under which the electric power industry (represented by NERC) writes its own compliance standards and FERC has limited ability require those standards be made more robust.

As a result, the decision of how much grid protection is enough grid protection to safeguard the American people from catastrophe is currently being left to *the electric power companies*. This clearly has to change, therefore I am strongly supporting this Foundation for Resilient Societies petition.

Thank you for considering these comments.
Fred A. Reitman, Ph.D., DABT

Document Content(s)

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE BONNEVILLE POWER ADMINISTRATION

On December 21, 2017, the Federal Energy Regulatory Commission (the "Commission") issued a Notice of Proposed Rulemaking ("NOPR") proposing to direct the North American Electric Reliability Corporation ("NERC") to develop and submit modifications to the NERC Reliability Standards to broaden reporting requirements for Cyber Security Incidents.[1] The Bonneville Power Administration ("Bonneville") supports the Commission's proposed directive to improve Cyber Security Incident reporting, and submits these comments for the Commission's consideration.

Bonneville is a Federal power marketing agency established to market wholesale electric power from the Federal hydroelectric projects in the Pacific Northwest. Bonneville currently markets power from 31 Federal hydro projects and some non-Federal projects. Bonneville also operates over 15,000 miles of transmission lines—approximately 80% of the high-voltage transmission lines in the region. Bonneville provides transmission on an open-access basis. Bonneville's service territory is within the WECC footprint and covers Washington, Oregon, Idaho, western Montana, and portions of California, Nevada, Utah, and Wyoming. Bonneville's wholesale power customers include public utilities, public utility districts, municipal districts,

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

public cooperatives, investor-owned utilities, and a few large industrial customers. Bonneville is registered for multiple functions under the NERC registry, including as a Transmission Owner and Transmission Operator.

I. BACKGROUND

On January 13, 2017, the Foundation for Resilient Societies ("Resilient Societies") filed a petition with the Commission requesting enhanced protections from malware, including more rigorous cyber security incident reporting requirements. In the NOPR, the Commission concluded that no action is required for enhanced protections against malware, as current NERC Reliability Standards and efforts are sufficient to address Resilient Societies' concerns.[2] However, the Commission also found that the current Cyber Security Incident reporting threshold may be insufficient to reveal the true state of cyber related threats.

Currently, the Critical Infrastructure Protection (CIP) Reliability Standards only require reporting of successful attempts at compromising an entity's systems. This standard resulted in zero Reportable Cyber Security Incidents in 2015 and 2016, while other venues that track cybersecurity incidents, such as the Industrial Control Systems Cyber Emergency Response Team, logged multiple reportable incidents.[3] In addition, NERC itself has recognized that there may be a gap in the reporting obligations under the CIP Reliability Standards.[4] As a result, the Commission proposes to direct NERC to address the reporting gap by modifying the CIP Reliability Standards to include all attempts to compromise an entity's systems, not just successful attempts.

[2] *Id.* at P23.
[3] *Id.* at P28.
[4] *Id.* at P29.

II. COMMENTS

Bonneville agrees with the Commission that there is currently a gap in reporting of Cyber Security Incidents, and the supports the Commission's proposal to require enhanced reporting requirements in the CIP Reliability Standards. However, new Reliability Standards requirements must ensure that the information reported is useful and does not result in under and over reporting of information.

The current definition of a Reportable Cyber Security Incident only includes *successful* attempts to compromise or disrupt an entity's systems. However, information about certain attempts to compromise will likely better assist the industry in preventing successful cyber attacks. As a result, a broader definition of a Reportable Cyber Security Incident is warranted.

The current definition of a Cyber Security Incident provides:

> 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.[5]

That definition is a good starting point for what should be reportable, as it includes attempts to compromise or disrupt, but may be too broad and result in overreporting of information. It will be difficult to establish a one-size fits all standard to use as a reporting threshold, developing report content, and setting reporting timelines, as not all threats are the same. It will be left up to the Standards Drafting Team to come up with a workable definition that results in the appropriate amount of information to be reported that is consistent with existing reporting thresholds in other venues.

Bonneville also believes that modifications to the CIP Reliability Standards and the definition of a Reportable Cyber Security Incident is the appropriate means of closing the

[5] *Glossary of Terms Used in NERC Reliability Standards* (Jan. 31, 2018).

reporting gap. As an alternative, the Commission suggests using data requests pursuant to Section 1600 of the NERC Rules of Procedure.[6] Bonneville does not believe using data requests is an effective means of obtaining information about cyber incidents. Data requests under Section 1600 are one time requests for existing data, and is not the appropriate vehicle for ensuring ongoing reporting necessary to make data about Cyber Security Incidents effective. Cyber threats are constantly evolving, making timely reporting essential to learning from and countering such threats.

III. CONCLUSION

Bonneville supports the Commission's proposal to direct NERC to modify the CIP Reliability Standards to broaden reporting of Cyber Security Incidents.

DATED February 21, 2018.

Respectfully submitted,

/s/ Allen C. Chan
Allen C. Chan, Attorney
Bonneville Power Administration
Office of General Counsel – LT-7
P.O. Box 3621
Portland, OR 97208
Telephone: 503-230-3551
Facsimile: 503-230-7405
Email: acchan@bpa.gov

[6] NOPR at P36.

Document Content(s)

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 IDAHO POWER COMPANY

Idaho Power Company ("Idaho Power") submits these Comments regarding the Notice of Proposed Rulemaking issued by the Federal Energy Regulatory Commission ("Commission" or "FERC") in the above-captioned proceeding. *Cyber Security Incident Reporting Reliability Standards*, 161 FERC ¶ 61,291 (December 21, 2017) ("NOPR"). Idaho Power is an investor-owned utility with service territory in Idaho and Oregon and is required to comply with the Commission's regulations. The Commission seeks comment on its proposal to direct the North American Electric Reliability Corporation and the Commission-certified Electric Reliability Organization to develop and submit modifications to the Critical Infrastructure Protection (CIP) Reliability Standards to improve the reporting of cyber security incidents, including those incidents that might facilitate efforts to harm the reliability of the bulk electric system ("BES").

I. COMMENTS

The Commission seeks comment on its need for the information to be reported; whether the information will have practical utility; ways to enhance the quality, utility, and clarity of the information collected; and suggestions for methods to minimize the respondent's burden. While the Commission seeks comment on numerous proposed reforms, Idaho Power offers the following comments on the proposed reforms as provided herein. As a threshold matter, Idaho Power believes that the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") data cannot necessarily be used to set standards for BES data because ICS-CERT encompasses non-BES information.

A. **Cyber Security Incident Reporting Threshold**.

Idaho Power believes additional reporting requirements do not increase cyber security. While additional reporting can provide some visibility into the types of threats that entities face, additional administrative burdens such as reporting requirements reduce the finite resources that entities have to monitor and defend their critical infrastructure.

In addition, the Electronic Access Control or Monitoring Systems ("EACMS") should be excluded from any additional requirements and only BES Cyber Systems and associated devices should be included in any further reporting requirements. An EACMS device, by definition, does not have a direct impact on the BES but is intended to perform access control or monitoring for those systems that can control or impact the BES. Any additional reporting requirement should focus on the devices that can control or impact the BES.

B. **Content of Cyber Security Incident Reports**.

Idaho Power believes reporting requirements established by the Commission should be succinct and not overly burdensome to the entity. Thresholds of impact that make it clear when an entity should report an incident and categories of incidents (attack vector), that are defined for entities, should be listed. Providing clarity of when to report and what to report will reduce the burden to the entity if additional reporting requirements are added. The level of intrusion should not be added to reporting requirements as it can often be hard to explain on paper and is somewhat subjective and differs between entities. 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.

C. Timing of Cyber Security Incident Reports.

Because it can be difficult to determine what happened, timing can often vary significantly. Idaho Power is concerned that a reporting timeline requirement has the potential to lead entities to rush their processes in analyzing an event. If FERC implements a time frame for reporting, it should ensure that an entity has adequate time to analyze each event before the reporting deadline.

D. Information Collection Statement.

The Commission seeks comment on whether such reported information will have practical utility. Historically, Idaho Power has seen little value in analyzing reported information. Sharing with other entities via such a report is often quite delayed and, in many instances, the entity has received the information from other sources by that time. Idaho Power is concerned about the potential for subsequent requests for additional information and the burden it may pose to an organization.

II. CONCLUSION

Idaho Power submits these Comments for the Commission's consideration. For the reasons set forth above, Idaho Power requests the Commission consider its input regarding the proposed revisions.

Respectfully submitted this 22nd day of February 2018.

Julia A. Hilton, Senior Counsel
Idaho Power Company
1221 West Idaho Street (83702)
P.O. Box 70
Boise, Idaho 83707
Telephone: (208) 388-6117
jhilton@idahopower.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 22nd day of February 2018 I electronically served a true and correct copy of the within and foregoing COMMENTS OF IDAHO POWER COMPANY upon all parties listed on the official service lists provided on the Commission's website for Docket Nos. RM18-2-000 and AD17-9-000.

Christa Bearry

Christa Bearry, Legal Assistant

Document Content(s)

Michael Mabee
(516) 808-0883
CivilDefenseBook@gmail.com
www.CivilDefenseBook.com

February 23, 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18–2–000
Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, and Commissioner Powelson, and Commissioner Glick:

Background:

I am a private citizen who has taken it upon himself to study the vulnerabilities of the U.S. electric grid to a variety of threats. My research lead me to write a book about how communities can prepare for and survive a long term power outage.[1] It is a book that never should have had to be written. I'm a regular working American with a regular day-job, but in my spare time I work with several non-profit groups to raise awareness of the existential threats the United States faces vis-à-vis the threats to the electric grid. I continue to write extensively on the subject. It is an occupation I never should have had to have.

On January 13, 2017, the Foundation for Resilient Societies filed a petition for rulemaking[2] with FERC because the electric grid does not have sufficient cybersecurity protection. Not surprisingly, the electric industry objects and seems to try to assure us that everything is fine.

Threats to the Bulk Power System and Critical Infrastructure:

On March 28, 2017[3] the Senate Committee on Homeland Security and Governmental Affairs reported this about the critical infrastructure:

> *"The United States depends on its critical infrastructure, particularly the electric power grid, as all critical infrastructure sectors are to some degree dependent on electricity to operate. A successful nuclear electromagnetic pulse (EMP) attack against the United States could cause the death of approximately 90 percent of the American population. Similarly, a geomagnetic disturbance (GMD) could have equally devastating effects on the power grid."* (Page 6.)

And the previous year, the House held a hearing entitled: "Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?"[4] In this hearing, the Committee noted that:

> *"The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability 'to take down control systems that operate U.S. power grids, water systems and other critical infrastructure'."* (Page vii. Internal citations omitted.)

On February 12, 2013, President Obama[5] noted:

> "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

In 2008, the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack reported about the bulk power system:

> *"Electrical power is necessary to support other critical infrastructures, including supply and distribution of water, food, fuel, communications, transport, financial transactions, emergency services, government services, and all other infrastructures supporting the national economy and welfare. Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities."* (Page vii.)[6]

In fact, there have been over two decades of congressional hearings, federal reports and studies about the various threats to the U.S. electric grid.[7] Of the numerous hearings on threats to the critical infrastructures, below are a select few in which Congress examined the cyber threats to the grid:

- "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection." Hearing before the US House, Joint Hearing of the Subcommittee on Cybersecurity, Science, and Research and Development, and the Subcommittee on Infrastructure and Border Security of the Select Committee On Homeland Security, 108th Congress (September 2003). https://www.gpo.gov/fdsys/pkg/CHRG-108hhrg99793/pdf/CHRG-108hhrg99793.pdf (accessed February 22, 2018).
- "Cyber Security: US Vulnerability and Preparedness." Hearing before the US House, Committee on Science, 109th Congress (September 15, 2005). https://www.gpo.gov/fdsys/pkg/CHRG-109hhrg23332/pdf/CHRG-109hhrg23332.pdf (accessed February 22, 2018).

- “The Cyber Threat to Control Systems: Stronger Regulations Are Necessary To Secure the Electric Grid.” Hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) October 17, 2007. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg48973/pdf/CHRG-110hhrg48973.pdf (accessed February 22, 2018).
- “Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid.” Hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (110th Congress) May 21, 2008. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg43177/pdf/CHRG-110hhrg43177.pdf (accessed February 22, 2018).
- “Securing the Modern Electric Grid from Physical and Cyber Attacks.” Hearing before the US House, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, 111th Congress (July 21, 2009). https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg53425/pdf/CHRG-111hhrg53425.pdf (accessed February 22, 2018).
- “Cyber Security.” Hearing before the US Senate, Committee on Energy and Natural Resources, (112th Congress) May 5, 2011. https://www.gpo.gov/fdsys/pkg/CHRG-112shrg67362/pdf/CHRG-112shrg67362.pdf (accessed February 22, 2018).
- “The EMP Threat: Examining the Consequences.” Hearing before the Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Serial No. 112-115. (112th Congress) September 12, 2012. https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg80856/pdf/CHRG-112hhrg80856.pdf (accessed February 22, 2018).
- “Cyber Threats and Security Solutions.” Hearing before the US House Committee on Energy and Commerce. (113th Congress) May 21, 2013. https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg82197/pdf/CHRG-113hhrg82197.pdf (accessed February 22, 2018).
- “Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?” Hearing before the House Subcommittee on Economic Development, Public Buildings, and Emergency Management. (114th Congress) April 14, 2016. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf (accessed February 22, 2018).

There is no debate that a loss of the electric grid for a long period of time, for any reason, would be catastrophic for the United States. Because we cannot support our present human population without the electric grid, the loss of life would be unimaginable. Here are the undisputed facts:

1. Fact: We know that cyber threats to the U.S. electric grid exist and are increasing.[8]

2. Fact: We know that the electric grid in the Ukraine was attacked and taken down twice by cyberattacks.[9]

3. Fact: We know that cyber-attacks have been known to destroy equipment.[10]

4. Fact: We know that all U.S. critical infrastructures are dependent on the bulk power system.[11]

Therefore, the cyber threat to the bulk power system represents an existential threat to the United States. The federal government – not the electric industry – is responsible for protecting against threats to national security. Therefore, the electric industry's objections to more stringent regulations are unpersuasive. The bulk power system must, without fail, be protected.

It is critical that the federal government insure that the critical infrastructures are adequately protected against known threats. In this case, the cyber security of the U.S. bulk power system is not a matter of convenience; it is a matter of paramount importance for the federal government.

Conclusion:

I urge you to require NERC to promulgate strict cybersecurity standards and reporting requirements. Thomas Jefferson famously said: "The first duty of government is the protection of life, not its destruction. Abandon that, and you have abandoned all."

FERC's duty here is clear. You must protect life. The threats to the electric grid constitute a national security issue. This is not a matter of a benevolent government being friendly to businesses. This is a matter of national security and the very real threat to millions of Americans' lives.

Respectfully submitted by:

Michael Mabee

[1] Mabee, Michael. *The Civil Defense Book: Emergency Preparedness for a Rural or Suburban Community*. ISBN-13: 978-1974320943, first edition published July 4, 2013, second edition published October 17, 2017.
[2] Foundation for Resilient Societies. "Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System." Filed January 13, 2017. https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/resilient_societies_petition_for_rulemaking_ad17-9.pdf (accessed February 22, 2018).
[3] Senate Report 115-12. Activities of the Committee on Homeland Security and Governmental Affairs. (115th Congress) March 28, 2017. https://www.gpo.gov/fdsys/pkg/CRPT-115srpt12/pdf/CRPT-115srpt12.pdf (accessed February 22, 2018).
[4] House Hearing before the Subcommittee on Economic Development, Public Buildings, and Emergency Management. *"Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure Of The Electrical Grid?"* (114th Congress) April 14, 2016. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf (accessed February 22, 2018).
[5] Executive Order 13636 *Improving Critical Infrastructure Cybersecurity.* February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed February 23, 2018).
[6] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *"Critical National Infrastructures."* 2008. https://permanent.access.gpo.gov/LPS101707/A2473-EMP_Commission-7MB.pdf (accessed February 23, 2018).
[7] See a comprehensive listing of these federal documents here: https://michaelmabee.info/government-documents-emp-and-grid-security/ (accessed February 22, 2018).
[8] RTO Insider. *Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities*. https://www.rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/ (accessed February 22, 2018).
[9] Wired magazine. *'Crash Override': The Malware That Took Down a Power Grid.* https://www.wired.com/story/crash-override-malware/ (accessed February 22, 2018).

[10] Wired Magazine. *An Unprecedented Look at Stuxnet, The World's First Digital Weapon*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed February 22, 2018).

[11] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *"Critical National Infrastructures."* 2008. https://permanent.access.gpo.gov/LPS101707/A2473-EMP_Commission-7MB.pdf (accessed February 23, 2018). Page vii.

Document Content(s)

23 February 2018

Chairman Kevin J. McInyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18-2-000
Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commisisoner Chatterjee, Commissioner LaFleur, Commissioner Powelson and Commissioner Glick:

As a private citizen living in the area of the United States with the highest electricity rates, I have spent many hours researching the electric grid. In doing so, the vulnerability of our electric grid to threats, specifically Electro Magnetic Pulse, both natural and man induced has surged to the top of my concerns.

It amazes and confounds me that for well over half a century the Federal government has had knowledge of this threat to the electric grid and yet the vast majority of the populace remains unprotected. Lives are at stake in astronomical numbers and yet the threats continue to grow and despite decades of study the vulnerability of the people remains unprotected. This is simply unacceptable.

I urge you to stop passing this "hot potato" from study to study and require the North American Electric Reliability Corporation to establish strict cyber security standards and reporting requirements with hefty suggestions of penalties for non-compliance no later than 30 June 2018. It is time for action. Potentially about 300 million American lives are at stake.

Respectfully submitted,

Karen Testerman

Karen Testerman

Document Content(s)

Douglas E. Ellsworth
301 Oakland Avenue
Council Bluffs, Iowa 51503

February 25, 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18–2–000, Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, and Commissioner Powelson, and Commissioner Glick:

I am concerned with the inadequacy of the existing cyber security incident reporting standards, and request that the Commission, with the authority under Section 215(d)(5) of the Federal Power Act, require the North American Electric Reliability Corporation (NERC) to address these inadequacies.

Among the warnings given since 2014 are:

- Testimony before the U.S. House Select Intelligence Committee from Admiral Mike Rogers, Director, National Security Agency and Commander, U.S. Cyber Command;

- The "Operation Cleaver" report of Cylance;

- The cyber-incident against the Ukrainian power grid of December, 2015 which caused nearly a quarter-million electric customers to lose power.

- The release of a Joint Analysis Report of the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) entitled "GRIZZLY STEPPE – Russian Malicious Cyber Activity" which describes a family of malware known as "Black Energy." The release of this document is particularly condemning of existing NERC Cyber standards because Black Energy was previously known, according to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the DHS, to exist in the U.S. energy sector.

- The publication "CRASHOVERRIDE – Analysis of the Threat to Electric Grid Operations" written by the private security firm Dragos. This publication views the Ukrainian grid exploit of 2016 from a viewpoint of an "insider" aligned with the ESET Slovak anti-virus firm. This

> document also evidences the disconnect in grid security that comes from an IT security firm accepting Industry's conceptualization of minimal long-term damage to systems, and minimizing the potential for long-term blackout.

The evidence list is long, and unfortunately, growing.

Perhaps the most important factor is the practice of increasingly more sophisticated malware to leverage Industrial Control Systems against themselves, prolonging the outage for an indefinite period of time. Physical override of SCADA systems can mitigate this condition where it is available, else manual instructions to SCADA will be ignored and ineffective.

The Commission should order NERC to include the fourteen recommended items listed by the Foundation for Resilient Societies in its *Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System* (Docket Number AD17-9).

Respectfully submitted,

Douglas E. Ellsworth

Document Content(s)

February 24, 2018

Chairman Kevin McIntyre
Commissioner Neil Chatterjee
Commissioner Richard Glick
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM 18-2, Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre and Commissioners Chatterjee, Glick, LaFleur, and Powelson,

I am a member of InfraGard, a 501(c) (3) public private partner with the FBI with about 47,000 members and am the Chairman of the InfraGard Electromagnetic Pulse Special Interest Group (EMP SIG™), with more than two thousand members with various specialty skills relating to critical. infrastructure protection and recovery. In addition, I am the lead editor and one of 24 coauthors of the December 2016 book: "*Powering Through: From Fragile Infrastructures to Community Resilience*." I am submitting this letter as a concerned citizen in my individual capacity and as President of the MDL Strategic Solutions, LLC.

Resilience of the U.S. electric power grid is vital to the country. It is a national imperative and critical in the light of foreign cyber intrusions and the North Korea threats to employ high altitude electromagnetic pulse (HEMP) weapons against the United States or its territories. If the grid were to be made truly resilient, then our adversaries might realize that assaults on the grid would no longer be an attractive class of threats or an effective way to attack our country.

I am in support of the rulemaking to report all cyber incidents to the Electricity Information Sharing and Analysis Center (E-ISAC) and to the Industrial Control System Cyber Emergency Response Team (ICS-CERT). In addition, I believe it would be prudent to report all incidents to the United States Cyber Emergency Response Team (US-CERT). If all incidents are reported to these organizations, they may be able to detect patterns and alert the utilities before something can be a widespread attack on the grid. Also, there is concern that a cyber attack could be a precursor to a HEMP attack.

Ideally, I am in agreement with the Foundation for Resilient Societies' request that all malware that is detected should be removed so that foreign adversaries would not be able to carry out an attack at a later date.

Respectfully submitted by:

Mary D. Lasky, President, MDL Strategic Solutions, LLC
mary.lasky@jhuapl.edu

Document Content(s)

February 26, 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18-2-000 Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, Commissioner Powelson and Commissioner Glick:

My name is Joe Weiss. I am submitting these comments as the Managing Director of Applied Control Solutions, LLC and focusing on the disclosure deficiencies in the NERC CIPs.

My background in the area of control system cyber security of the electric grid is extensive and represents almost 19 years of working in control system cyber security including several years as a subject matter expert in control system cyber security to FERC. As background, I helped start the control system cyber security program for the electric utilities in 2000 while at the Electric Power Research Institute (EPRI); supported the Idaho National Laboratory (INL) in establishing the SCADA Test Bed; supported the National Institute of Standards and Technology (NIST) in extending NIST 800-53 to include control systems; supported the Pacific Northwest National Laboratory (PNNL) in support of the Nuclear Regulatory Commission (NRC) on development of Regulatory Guide 5.71 (Cyber Security for Nuclear Plants); supported FERC as a subject matter expert; supported the Department of Defense (DOD) as a subject matter expert with a focus on the Aurora vulnerability; and supported the International Atomic Energy Agency (IAEA) on scenario-based training for nuclear plants. ***Applied Control Solutions, LLC has amassed a database of more than 1,000 actual control system cyber incidents with more than 250 being in the North American electric system.*** Contemporarily, I serve as the Managing Director of the International Society of Automation (ISA)99 – the international standards on control system cyber security. On February 23, 2016, I gave the keynote to the National Academy of Science, Engineering, and Medicine addressing control system cyber security. Also, I am the author of a treatise on safeguarding industrial control systems– Protecting Industrial Control Systems from Electronic Threats.

The current CIP Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning), requires incidents to be reported only if they have compromised or disrupted one or more reliability tasks. FERC is concerned this threshold may understate the true scope of cyber-related threats facing the grid. In particular, the lack of any reported incidents in 2015 and 2016 suggests a gap in the current mandatory reporting requirement. The 2017 State of Reliability report by the North American Electric Reliability Corp. (NERC), which is responsible for enforcing FERC-approved mandatory reliability standards, echoed this concern.

This Notice of Proposed Rulemaking (NOPR) would direct NERC to submit modifications to broaden the requirement to include mandatory reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems (EACMS). In addition, the proposal would require NERC to modify the CIP Reliability Standards to:

- Specify the required information in cyber security incident reports to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; and

- Establish a deadline for filing a report once a compromise or disruption, or an attempted compromise or disruption, is identified by a responsible entity.

The purpose of addressing cyber security in the electric industry is to reduce the potential impact on grid reliability not to find malware. The NIST definition of a cyber incident is electronic communications between systems that affect Confidentiality, Integrity, or Availability. The NIST definition does not mention the term "malicious". As demonstrated by the 2008 Florida outage, the impact of cyber incident can be the same whether it is malicious or unintentional. In the Florida case, the only difference between the incident being malicious versus unintentional was the motivation of the engineer in the substation. In either case, the event cascaded throughout the transmission system leaving almost 1 million customers without power for almost 8 hours and led to the loss of 22 transmission lines, 4,300 MW of generation, and 3,650 MW of customer service or load.

Many control system cyber incidents were not identified for months (December 2015 and 2016 Ukrainian cyber attacks) to even years (Stuxnet). Even more important, neither the "warhead" for Stuxnet nor Aurora was malware, but both could have VERY significant impacts on short and long-term grid reliability.

There are two issues that must be considered:

- There are no control system cyber forensics at the process sensor, actuator, or drive level (out-of-scope for NERC CIP). Yet, this is where damage to long lead-time, critical electric equipment can occur potentially resulting in very long-term, wide-spread outages.

- There is no training for control system engineers to recognize upset conditions may be control system cyber incidents (this was my work for IAEA). As an example, protective relay engineers need to be trained to identify Aurora-type events as Aurora is not malware that can be identified by IT.

The need for the NOPR is amply demonstrated by the lack of disclosure of obvious cyber-related events as being "cyber as can be seen from these sample 2015-2016 incidents.

"...As a result, the EMS lost communications with all RTUs."

"...caused false breaker status indications on a line relay, and this resulted in relay misoperation. The concurrent misoperation of six relays associated with multiple 525 kV breakers...."

"During a regularly scheduled firewall patch installation, an entity experienced multiple inter-control center communications protocol (ICCP) communication failures with external entities. The entity performed a patch update to its main control center (MCC) ICCP firewall resulted in an outage of ICCP communications for greater than 30 minutes, constituting a reportable event per EOP-004."

“An EMS was configured such that all nodes (e.g., servers, workstations) were prompted to reboot for a particular system condition. This complete system restart sequence took 47 minutes to complete. Consequently, there was a complete loss of control and monitoring functionality until each critical server and workstation reported its status as normal and fully functional.”

“SCADA alarms were not distinguishable between non-rolling blackout circuits and rolling blackout circuits. It became difficult for operators to identify and respond to the alarms and outages which were not generated by the rolling blackouts. Several circuits were not correctly identified as critical load, including hospitals and jails. Maps of area outages were not immediately available to meet the needs of management, stakeholders, and media. Communications processes were not fully defined or fully implemented with other local government agencies, local law enforcement, local emergency management teams, and other critical facilities.”

“A temporary rack-mounted uninterruptible power supply (UPS) failed, resulting in the loss of the RTU LAN, the loss of system visibility, and the failure of ICCP link for 50 minutes.”

In 2017, a utility lost all relay communications to almost 400 high voltage (230 and 500KV) relays – certainly a grid reliability concern. This event appeared to be similar to the CrashOverirde/Industroyer malware. However, the utility did not report this event as being cyber-related.

One of the most egregious examples of NERC’s refusal to identify events as being cyber-related was a Lessons-Learned issued December 29, 2015, soon after the 2015 Ukrainian cyber attack. A broadcast storm (denial of service) led to the control center losing monitoring and control of its portion of the Bulk Electric System for approximately 39 minutes. What’s more problematic given the timing of the Ukrainian cyber attack was NERC’s recommendation that “EMS/SCADA servers should prioritize traffic such that situational awareness traffic is prioritized over other network traffic, such as cyber security logging traffic.” This is in direct contradiction to almost all guidance, particularly following the 2015 Ukrainian cyber attack, that monitoring cyber security network traffic is critical.

Consequently, I recommend the FERC recommendations be expanded to include the following:

- Require utility personnel to identify all electronic communication impacts that could affect grid reliability as being cyber-related, whether malicious or unintentional.

- Require utilities not NERC, to disclose to FERC, ICS-CERT, the National Cybersecurity and Communications Integration Center (NCCIC) and the utility industry all control system cyber incidents in plant, transmission, distribution, or SCADA operations in an expeditious manner. This is because many cyber-related events are not unique to just one utility or facility.

- Require training by plant and substation staff to better understand control system cyber security and to recognize upset conditions that could be cyber-related.

- Require utility IT and physical Security Operation Centers (SOCs) to coordinate with plant and substation Operation Centers to better coordinate what upset conditions may be cyber-related.

Respectfully,

Joseph Weiss PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC
Managing Director ISA99

AC
APPLIEDCONTROLSolutions

Document Content(s)

U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

February 26, 2018

Kimberly Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Subject: ***Cyber Security Incident Reporting Reliability Standards*** **(Docket No. RM18-2-000)**

Dear Secretary Bose:

The U.S. Chamber of Commerce welcomes the opportunity to respond to the Federal Energy Regulatory Commission's (FERC's) request for comments on its notice of proposed rulemaking *Cyber Security Incident Reporting Reliability Standards*.[1]

The Chamber respects FERC's interest in obtaining an accurate picture of cyber risks that could impact the reliable operation of the bulk electric system (BES). North American Electric Reliability Corporation (NERC) entities also need quality, timely cyber threat data, some of which are only obtainable from governmental sources. Our organization strongly supports voluntary, protected cybersecurity information-sharing programs. It believes that FERC should resist calls to direct NERC to modify the Critical Infrastructure Protection (CIP) Reliability Standards to compel more reporting by industry.

Nevertheless, the Chamber believes that a positive outcome is achievable between FERC and NERC stakeholders. Instead of mandating additional reporting, FERC should explore opportunities with industry to support the existing voluntary cybersecurity information-sharing programs. An optimal and sustainable outcome would contain the following principles and objectives:

- **Mandatory cyber incident reporting does not strengthen cybersecurity.** More forced reporting is likely to create substantial noise in the system and lead to a diffusion of NERC members' limited resources toward compliance and away from risk management activities.[2]

- **Information sharing needs to be rooted in reciprocity.** NERC and industry parties should voluntarily exchange threat data concerning potential and actual cyberattacks. Information sharing should be a two-way street—one where threat data flow *to businesses from government* and vice versa. The agency's rulemaking does not address how reported cyber information would tangibly benefit electric utilities and other industry actors.

- **NERC entities should have reasonable control over the handling of shared threat information.** Designations (e.g., the Traffic Light Protocol) identify unclassified information that may not be suitable for public release and could require special handling.[3]

- **Electric-sector parties need security clearances.** Despite a well-known backlog in the security clearance process, many electric-sector entities that are covered by the CIP standards need security clearances. FERC's proposed rulemaking does not account for how the agency's call for enhanced information is at odds with the incredibly slow background investigation process.[4]

- **NERC stakeholders need access to classified threat data and closer collaboration with federal agencies and industry peers.**[5] Private parties, put simply, need to become a customer of the intelligence community (IC) as part of an overall solution to boosting U.S. cybersecurity. Electric-sector entities must be able to receive classified threat information in real time and coordinate securely with government and other private companies on network defense.[6] Increasing productive interactions between self-selected industry actors and the IC regarding cybersecurity is a top Chamber objective.

- **FERC actions should foster, not impede, industry's use of leading cyber technologies.** The agency's suggested regulatory changes could slow innovative approaches to cybersecurity among electric utilities, which would be troubling to the Chamber. NERC entities may opt to leverage technology vendors (e.g., cloud computing providers) to improve service operations and reliability for functions that may not operate BES directly but integrate closely with such systems and could be considered an extension of electricity providers.[7]

- **Public-private response coordination needs tightening.** NERC entities need confidence that public and private stakeholders are clear about their roles and responsibilities. The Chamber recognizes that cyberattacks cannot be handled solely by government, but cyberspace is the only domain where the government asks private companies to defend themselves against foreign powers and other significant threats, which is unworkable in many instances.[8]

***

The Chamber appreciates the opportunity to offer its views to FERC on constructive ways to address cybersecurity incident reporting. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com, 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Ann Beauchesne

Ann M. Beauchesne
Senior Vice President

Matthew J Eggers

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Endnotes

[1] www.federalregister.gov/documents/2017/12/28/2017-28083/cyber-security-incident-reporting-reliability-standards

www.ferc.gov/media/news-releases/2017/2017-4/12-21-17-E-1.asp#.WoCvVUly6Uk

[2] www.gao.gov/products/GAO-08-904T

www.uschamber.com/sites/default/files/documents/files/oct_20_letter_to_wh_cyber_commission_re_sec_pritzker_address_final.pdf

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[4] www.gao.gov/products/GAO-18-29?utm_medium=email&utm_source=govdelivery

[5] www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

[6] http://docs.house.gov/meetings/HM/HM08/20171115/106632/HHRG-115-HM08-Wstate-KnakeR-20171115.pdf

www.insaonline.org/wp-content/uploads/2017/06/INSA-FINnet-Proposal-June-2017.pdf

http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Bio-HealeyJ-20170301-U1.pdf

www.congress.gov/bill/114th-congress/senate-bill/3017

www.congress.gov/bill/115th-congress/senate-bill/133

www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

[7] Prior to introducing modifications to the CIP standards, FERC should convene NERC stakeholders and the vendor community. This group could discuss the anticipated impacts of the rulemaking, the agency's desired outcomes, and the capabilities and investments of both regulated entities and third-party providers. Such a dialogue would provide an alternate way to achieve FERC's desired outcomes.

[8] www.uschamber.com/sites/default/files/documents/files/10-31-16_uscc_letter_re_draft_ncirp_final.pdf

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

	)	
	)	
Cyber Security Incident	)	Docket No. RM18-2-000
Reporting Reliability Standards	)	
	)	
	)	

COMMENTS OF INTERNATIONAL TRANSMISSION COMPANY d/b/a ITC*TRANSMISSION*, MICHIGAN ELECTRIC TRANSMISSION COMPANY, LLC, ITC MIDWEST LLC, AND ITC GREAT PLAINS, LLC

International Transmission Company d/b/a ITC*Transmission*, Michigan Electric Transmission Company, LLC, ITC Midwest LLC, and ITC Great Plains, LLC (collectively, “ITC” or “ITC Companies”) respectfully submit these comments in response to the Federal Energy Regulatory Commission’s (“Commission’s”) December 21, 2017, Notice of Proposed Rulemaking issued in the above-captioned proceeding.[1] ITC previously moved to intervene and filed comments in Docket No. AD17-9-000 on February 17, 2017.

I. BACKGROUND

On January 19, 2017, in Docket No. AD17-9-000, the Foundation for Resilient Societies (“FSR”) submitted a petition requesting that the Commission initiate a rulemaking proceeding which would direct the North American Electric Reliability Corporation (“NERC”) to submit a Reliability Standard establishing requirements for malware detection, reporting, mitigation, and removal. In response to comments submitted by NERC, ITC, and other parties, the Commission

[1] 161 FERC ¶ 61,291 (2017) (“NOPR”).

has declined to act on the petition in the manner requested by FSR, and has terminated Docket No. AD17-9-000.[2]

In so doing, however, the Commission has also proposed to direct NERC to develop modifications to the CIP Reliability Standards to improve the mandatory reporting of Cyber Security Incidents. In support of its proposed directive, the Commission cites the 2017 NERC State of Reliability Report, which found that were no incidents that met the NERC definition of Reportable Cyber Security Incident during that year. Noting that many cyber threats facing the electricity industry exist which, despite having the potential to cause serious impacts, nonetheless do not meet the existing definition of Reportable Cyber Security Incident, the Report recommends that this definition be refined "to be more granular and include zero-consequence incidents that might be precursors to something more serious."[3] To that end, the Commission has proposed to direct NERC to modify the Cyber Security Incident reporting threshold, the information to be included in Cyber Security Incident reports, and the timing of Cyber Security Incident reports.

a. Cyber Security Incident Reporting Threshold

In the first element of its proposed directive, the Commission proposes to require NERC to modify the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter ("ESP") or associated Electronic Access Control or Monitoring Systems ("EACMS"). Presently, the 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

[2] NOPR at P 23.

[3] *Id*. at P 22 (internal citations omitted).

Perimeter or Physical Security Perimeter or Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."[4] A Reportable Cyber Security Incident, however, is then defined in the NERC Glossary as "[a] Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."[5] The Commission notes that, in contrast to the lack of any Reportable Cyber Security Incidents over the past three years, both the Department of Energy and the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") recorded multiple cybersecurity incidents during that time. Thus, the Commission's directive would lower the threshold for "Reportable Cyber Security Incident" to include a "compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS."[6] With respect to this directive, the Commission specifically seeks comment on whether to "exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold."[7]

b. Cyber Security Incident Report Contents

As the Commission notes, currently-effective Reliability Standard CIP-008-5, Requirement R1, Part 1.2 requires that a responsible entity provide an initial notification of a Reportable Cyber Security Incident to the E-ISAC within one hour of the determination that a Cyber Security Incident is reportable, unless prohibited by law, but does not specify the contents of the report.[8]

[4] *Id*. at P 27.

[5] *Id*.

[6] *Id*. at P 30

[7] *Id*. at P 36.

[8] *Id*. at P 37.

The NOPR proposes to direct NERC to specify that a Cyber Security incident report submitted to the Electricity Information Sharing and Analysis Center ("E-ISAC") must include

1. The functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve;
2. The attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and
3. The level of intrusion that was achieved or attempted as a result of the Cyber Security Incident.[9]

c. Cyber Security Incident Report Timing

In addition to not specifying the contents required of a Cyber Security Incident report, CIP-008-5 also fails to specify a timeframe after initial E-ISAC notification in which an entity must subsequently complete a full Cyber Security Incident report. The Commission therefore proposes to direct NERC to establish requirements outlining deadlines for filing a Cyber Security Incident Report once a compromise or disruption to reliable bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity.[10] The Commission's proposal would also require Reports to be submitted to the E-ISAC and ICS-CERT.[11] Additionally, the Commission proposes to direct NERC to file annually an anonymized report providing an aggregated summary of the reported information.[12]

II. COMMENTS

a. Cyber Security Incident Reporting Threshold

[9] *Id*. at P 38.

[10] *Id*. at P 41.

[11] *Id*. at P 42.

[12] *Id*.

While ITC generally concurs with the Commission’s finding that the current Cyber Security Incident reporting threshold fails to capture an appropriately broad swath of cybersecurity incidents necessary to timely identify threats to the reliable operation of the Bulk Electric System, ITC respectfully requests that the Commission refrain from including unsuccessful attempts to compromise an ESP-associated EACMS in the revised definition of reportable Cyber Security Incident. As the Commission is no doubt well-aware, responsible entities, like most any entity that maintains networks with publicly-visible IP addresses, face a near constant barrage of attempts to compromise its systems. In particular, responsible entities 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. A Standard which would classify these types of attempted-but-unsuccessful attacks as Reportable Cyber Incidents would lead only to the generation of reams of reports which provide little, if any, enhancement to the ability of NERC and other responsible entities to identify and respond to emerging cyber security threats. As proposed, the Commission’s directive to include attempted compromises of ESP-associated EACMS would appear to require reporting for a sizable number of these common events.

As such, in response to the Commission’s solicitation of comments on this proposal, while ITC 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. Doing so will effectively balance the need to capture additional cybersecurity incidents which could facilitate subsequent efforts to harm the reliable operation of the bulk electric system through breaches of an ESP with the need to avoid generating vast amounts of reports of attempted EACMS breaches which pose little objective threat to the integrity of an entity's operations, and which may, by virtue of their sheer number, actually inhibit the ability of NERC to identify more serious threats. Due to increases in the resilience of ESPs to direct attack, ITC has seen a relative increase in attempts to breach its corporate networks in a manner which could facilitate subsequent attacks on systems within ESPs; for example, social engineering attacks which seek to obtain credentials for accessing BES Cyber Assets protected by ESPs and bitcoin mining activity. Therefore ITC agrees that any successful breach of a corporate network, while perhaps not a direct threat to the reliable operation of an entity's BES Cyber Assets, should nonetheless be classified as reportable.

b. Cyber Security Incident Report Contents

ITC supports the Commission's proposal as a reasonable set of baseline requirements for reporting. ITC does harbor concerns that, while facially anonymous, the collective information which would be required under the Commission's directive could permit other parties to determine the identity of the reporting entity based on indicators which can be matched to an entity's publicly-known characteristics. To that end, ITC will work within the NERC stakeholder and standards development processes to ensure that the Standards submitted in response to the Commission's final rule are structured to preserve anonymity to the maximum extent practicable.

c. Cyber Security Incident Report Timing

With respect to the Commission's proposal to also require Reports to be submitted to the E-ISAC and ICS-CERT, the Commission should limit required reports to ICS-CERT to only incidents which impact industrial control systems within ICS-CERT's purview. ITC would submit that the definition of industrial control systems promulgated by the National Institute of Standards and Technology ("NIST") would serve as a useful threshold for mandatory ICS-CERT reporting.[13]

Additionally, ITC requests that the Commission clarify its proposal that "the reports submitted under the enhanced mandatory reporting requirements would be provided to E-ISAC, similar to the current reporting scheme, as well as ICS-CERT. The detailed incident reporting would not be submitted to the Commission."[14] Specifically, does the Commission intend that only the final report be submitted also to the ICS-CERT, or that initial reports must be provided, as well? ITC would note 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.

III. CONCLUSION

WHEREFORE, for the reasons discussed herein, ITC respectfully asks the Commission to act in manner consistent with the foregoing.

Respectfully submitted,

/s/ James W. Bixby
James W. Bixby
ITC Holdings Corp.
601 Thirteenth Street N.W.
Suite 710S

[13] *See* NIST, *Guide to Industrial Control Systems (ICS) Security*, Special Publication 800-82, at 2-1 (May, 2015) (*available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*).

[14] NOPR at P 41.

Washington, DC 20005
jbixby@itctransco.com

Counsel for the ITC Companies

February 26, 2018

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

	)	
	)	
Cyber Security Incident	)	Docket No. RM18-2-000
Reporting Reliability Standards	)	
	)	
	)	

CERTIFICATE OF SERVICE

I hereby certify that I have caused a copy of the foregoing document to be served on each person designated on the official service list compiled by the Secretary of the Commission in this proceeding on this 26th day of February, 2018.

/s/ James W. Bixby
James W. Bixby
Counsel – Regulatory & Legislative
ITC Holdings Corp.
601 Thirteenth Street N.W.
Suite 710S
Washington, DC 20005

Counsel for the ITC Companies

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Critical Infrastructure Reliability Standards) Docket No. RM18-2-000

COMMENTS OF ARIZONA PUBLIC SERVICE COMPANY

Arizona Public Service Company ("APS") submits comments regarding the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking ("NOPR") issued on December 21, 2017, in the above captioned docket.[1] As described below, APS supports the Commission's objectives to improve awareness of existing and future cyber security threats and potential vulnerabilities; however, for several reasons described below, the Commission's proposal may not meet its intent. To better ensure that the Commission, entities responsible under the Critical Infrastructure Protection reliability standards ("CIP Standards") (hereinafter "Responsible Entities"), and the North American Electric Reliability Corporation ("NERC") become aware of cyber security risks and vulnerabilities timely and have an accurate understanding of such risks and vulnerabilities, APS suggests modifications to the Commission's proposal that will leverage existing reporting processes and ensure that the information that is most valuable to these entities relative to cyber security risks is accurately and efficiently conveyed in a timely and actionable manner.

I. INTRODUCTION AND OVERVIEW

[1] Cyber Security Incident Reporting Reliability Standards, Notice of Proposed Rulemaking, 161 FERC ¶ 61,291 (December 21, 2017).

APS, a wholly-owned subsidiary of Pinnacle West Capital Corporation, is a vertically integrated public utility doing business under the laws of the State of Arizona, and is engaged in generating, transmitting, and distributing electricity in eleven of Arizona's fifteen counties. APS serves more than one million retail electric customers and participates in wholesale markets throughout the Western Interconnection. APS owns generation that has the ability to generate approximately 6,500 megawatts with its diverse portfolio of nuclear, coal, gas combustion and combined cycle turbines, wind, and solar generating units. APS is registered with NERC for twelve registered functions, including Planning Coordinator, Transmission Planner, Transmission Owner and Generation Owner.

In the NOPR, the Commission is proposing to direct NERC, the Commission-certified Electric Reliability Organization, to develop and submit modifications to the CIP Standards to expand the scope for mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System ("BES"). More specifically, the Commission is proposing to direct NERC to develop modifications to the CIP Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's Electronic Security Perimeter ("ESP"), but not its associated Electronic Access Control or Monitoring Systems ("EACMS"), to specify the required information included in Cyber Security Incident reports, and to establish a deadline 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 Commission seeks comment on this proposal, including:

- Whether to exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold;
- The appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities; and
- The appropriate timing for Cyber Security Incident reporting to better ensure timely sharing of information and thereby enhance situational awareness.

The Commission also seeks comment on potential alternatives to modifying the mandatory reporting requirements in the CIP Standards including whether a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure ("ROP") would effectively address the reporting gap and current lack of awareness of cyber-related incidents discussed in the NOPR and satisfy the goals of the proposed directive.

In addition to the modifications to the CIP Standards proposed in the NOPR, the Commission proposed to continue having the reports go to the Electricity Information Sharing and Analysis Center ("E-ISAC") and to require that reports also be sent to the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"). The NOPR further proposed to direct NERC file an annual, public, and anonymized summary of the reports. The Commission sought comment on both of these proposals.

II. APS COMMENTS

Although APS supports Responsible Entities, NERC, and the Commission being aware of existing and future cyber security risks and potential vulnerabilities as soon as possible, there may be a more efficient or effective manner in which to address the Commission's concerns and satisfy the Commission's objectives expressed in the NOPR. In particular, the Commission states that its concerns arise from the perception that the current "mandatory reporting process does not create an accurate picture of cyber security risk …."[2] It noted that NERC indicates that, "… there were no reportable cyber security incidents during 2016…." while, in contrast, the 2016 annual summary of DOE's Electric Disturbance Reporting Form OE-417 contained four cybersecurity incidents reported in 2016: two suspected cyber attacks and two actual cyber attacks, and the ICS-CERT responded to fifty-nine cybersecurity incidents within the Energy Sector in 2016.[3] Finally, APS notes that these reports are not necessarily indicative that the level of cyber and/or physical attacks are specifically targeting those assets that would be subject to the CIP Standards. In fact, in APS's experience, the majority of the cyber attacks are occurring in the corporate environment – not in those environments that are subject to the CIP Standards.

While the existing mandatory reporting under the CIP Standards may not, as written, satisfy the Commission's objectives as stated in the NOPR, the Commission itself has noted that the exact information that the Commission is seeking is

[2] *Id*. at P10.

[3] *Id*. APS also notes that the Energy sector for ICS-CERT is comprised of three segments: electricity, oil, and natural gas and the reporting referenced is a summary report that likely includes incidents that occurred outside of the Electric sub-sector. (*See* https://www.dhs.gov/energy-sector)

available from at least one other mandatory reporting obligation. There have long been efforts to streamline reporting efforts under the NERC reliability standards where there is an existing, additional mandatory reporting requirement such as the Electric Disturbance Events, Form OE-417, reports ("Form OE-417"). The goal of such efforts has been to reduce redundant reporting obligations to ensure that the value of the reporting is not adversely impacted by numerous different and potentially conflicting reporting obligations. Redundant reporting obligations for potential cyber security events would be very onerous for the industry and the value added would be minimal since the data being collected via the additional reporting obligation is already being collected. APS, in its comments, discusses this issue and potential alternative approaches below.

A. APS Does Not Support The Commission's Proposal To Modify The CIP Standards To Include, In Mandatory Cyber Security Incident Reporting, Incidents That Did Not Cause Any Harm, But Could Facilitate Subsequent Efforts To Harm The Reliable Operation Of The BES.

APS supports the Commission's objectives expressed in the NOPR; however, it disagrees that the solution is to modify the CIP Standards to include the mandatory reporting of Cyber Security Incidents that attempt to compromise a Responsible Entity's ESP or associated EACMS. APS believes that such modification would result in a redundant reporting obligation and respectfully suggests that the Commission instead 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 the ICS-CERT. Such an alternative approach would ensure consistency in data being reported to the various regulatory agencies and would leverage existing reporting obligations to satisfy the Commission's objective, which is to ensure that it, NERC, and Responsible Entities receive information regarding existing and future cyber security risks and potential vulnerabilities as soon as possible.

More specifically, APS notes that the Form OE-417 Form requires "Balancing Authorities, Reliability Coordinators, some Generating Entities, and Electric Utilities" to report:

> 9. Physical attack that ***could potentially impact electric power system adequacy or reliability***; or vandalism which targets components of any security systems
>
> 10. Cyber event that ***could potentially impact electric power system adequacy or reliability***[4] (Emphasis Added) within six hours of the incident, with a final report submitted within 72 hours of the incident. The Form OE-417 defines Physical Attack and Cyber Event as follows:
>
> Physical Attack: An attack on any part of your system suspected of being a deliberate attack or sabotage that disrupts system operations or had the intent to harm the national security of the United States. …
>
> Cyber Event: 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.[5]

APS notes that the population of entities subject to mandatory reporting of Form OE-417 is essentially the same as the population of Responsible Entities responsible for reporting under the CIP Standards. Further, the requirement to report a physical attack or cyber event that could potentially impact electric power system adequacy or reliability under the Form OE-417 would result in the reporting of the same or similar incidents as the reporting of incidents that did not cause any harm, but that could facilitate subsequent efforts to harm the reliable operation of the BES.

[4] Form OE-417 Electric Emergency Incident and Disturbance Report located at https://www.oe.netl.doe.gov/oe417.aspx.

[5] *Id*.

For these reasons, APS respectfully 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. Moreover, the reporting requirement that already exists under Form OE-417 is well-established and mandatory. It already collects and would, therefore, provide both detailed and summary information that would be useful to NERC, the Commission, and Responsible Entities. In fact, the provision of both a high-level summary and a detailed description as required in the Form OE-417 would allow receiving entities to: (1) rapidly triage incidents to determine if actions need to be taken for their systems; and (2) review and take action based upon detailed descriptions of the incident and the actions taken to resolve it should an incident be determined to be applicable to a Responsible Entity's systems.

Additionally, APS notes that there is precedent for leveraging existing reporting obligations to satisfy reporting obligations under the NERC Reliability Standards. More specifically, the measures for Requirement R2 of EOP-004-3 and Attachment 1 to EOP-004-3 contemplate the submission of the Form OE-417 to meet the obligation to report an event to the "…Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority)." Because the Form OE-417 is also required to be submitted for a physical attack or cyber event that could potentially impact electric power system adequacy or reliability, which is essentially the same as or similar to the Commission's "incidents that did not cause any harm but could facilitate subsequent efforts to harm the reliable operation of the BES," APS respectfully asserts that, rather than defining an entirely independent, redundant reporting obligation under the CIP Standards, the Commission consider directing NERC to add an obligation for Responsible Entities to submit to the E-ISAC and ICS-CERT any Form OE-417 that is submitted to meet the obligation for reporting a physical attack or cyber event that could potentially impact electric power system adequacy or reliability.

Such requirement would meet the Commission's objectives as expressed in the NOPR without adding the administrative burden of an entirely independent, redundant reporting obligation. Moreover, because of the six (6) hour submission time frame for the Form OE-417, this process would not over-burden entities administratively nor divert resources during critical event time periods, but would still allow important information to be timely distributed consistently. Hence, because there is already an existing reporting obligation for physical attacks or cyber events that could potentially impact electric power system adequacy or reliability, APS respectfully recommends that the Commission consider leveraging this existing process in a manner similar to that available to Responsible Entities pursuant to Requirement R2 of EOP-004-3 rather than directing NERC to create a new, redundant reporting obligation.

For these reasons, APS does not support the Commission's proposal to direct NERC to develop a new, independent reporting obligation; however, APS does support meeting the Commission's objectives through the leveraging of existing reporting processes, *e.g.*, by requiring broader distribution of Form OE-417 when it is submitted to report a physical attack or cyber event that could potentially impact electric power system adequacy or reliability.

B. APS Does Not Support The Commission's Proposal To Define Reporting Based On Inclusion Or Exclusion Of EACMS Or The ESP.

APS respectfully recommends that, as EACMS and ESP are currently defined, the proposal to include or exclude such assets could result in gaps in the reporting of incidents that did not cause any harm, but could facilitate subsequent efforts to harm the reliable operation of the BES. In particular, the Commission proposes to exclude EACMS while including the ESP. The Commission's proposal is silent regarding Electronic Access Points ("EAPs").

While APS concurs that the incidents impacting the ESP should certainly be in scope of reporting, it is concerned that the exclusion of EACMS (which includes EAPs) results in a likely compromise scenario going unreported. More specifically, a user's credentials to an Intermediate System, which includes/can be classified as an EAP(s) and/or EACMS, could be compromised. The point at which that compromise occurs would not implicate the ESP, but could impact or attempt to impact a BES Cyber Asset ("BCA") or System ("BCS"). These access-focused attack vectors are likely compromise scenarios for cyber events and the proposed scope of reporting would leave such scenarios unaddressed.

Conversely, there are numerous EACMS for which a compromise scenario would not be critical or allow potential access to an ESP, BCA, or BCS. As an example, there are assets that serve as EACMS, but that do not serve as EAPs to BCAs or BCS and that would not, therefore, have potential to cause harm to the BES or to facilitate subsequent efforts to harm the reliable operation of the BES. Additionally, there are EACMS that perform nothing more than monitoring functions. These assets cannot grant or reject access attempts and, therefore, cannot be utilized to access ESPs, BCAs, or BCS. These assets include firewalls that scan and reject significant traffic every minute of every day and assets such as log aggregators that passively record access attempts. While certain EACMS should be included in mandatory reporting, the wholesale inclusion of EACMS would result in the over-reporting of attempts to compromise that could not have the effect of causing harm to the BES nor the facilitation of subsequent efforts to harm the reliable operation of the BES. For these reasons, APS cannot support the Commission's proposal to exclude all EACMS nor can it support the inclusion of all EACMS.

However, it is important to recognize that both NERC and the industry have recognized the different functions of EACMS and are, as part of the current standards development process, evaluating the need to separate the function of Electronic Access Control from that of Electronic Access Monitoring. Until such evaluation is complete and modifications to the definition of EACMS are made, the current definition of EACMS will have the result of including devices that have no direct impact to the ESP, BCAs, or BCS in the scope of required reporting. The inclusion of those devices that only monitor electronic access, but do not control or otherwise grant access in mandatory reporting obligations would provide no value or benefit to NERC, the Commission, or Responsible Entities and would actually divert attention and resources from the review and triage of incident information that does have the potential to position entities to prevent or mitigate incidents that could cause harm to the BES and/or facilitate subsequent efforts to harm the reliable operation of the BES. Nonetheless, the exclusion of EACMS has the effect of excluding access attempts to the Intermediate System, which attempts are significant enough that they should be subject to mandatory reporting obligations.

For these reasons, APS cannot support the scoping recommended by the Commission until such time as the standards development processes that are currently evaluating the definition of EACMS have completed. While APS supports the Commission's objectives, at this time, the assets and classification are not sufficiently mature to achieve the value that the Commission seeks by including the ESP and excluding EACMS. Finally, as discussed above, the reporting obligation set forth in Form OE-417 would be an effective alternative to the Commission's proposal that would moot this issue.

C. APS Does Not Support The Minimum Set Of Attributes Proposed To Be Reported As These Attributes Will Not Achieve The Commission's Objectives.

In the NOPR, the Commission proposed a minimum set of attributes to be included as part of its overall reporting. In particular, the Commission proposed that every report submitted should be required to include: (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident. It is APS's position that, because each entity's network topology, architecture, applications, and other characteristics are different, any requirement to 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.

More specifically, the functional impact of an incident is easy to ascertain and could be provided in reporting, but, because one entity's architecture, applications, and security controls do not directly map or translate to another entity's architecture, applications, and security controls, the functional impact to one entity is a subjective, specific observation that is applicable only to that entity's systems and networks. Thus, it would add little value to awareness, transparency, or visibility and would likely not facilitate prevention of future attacks. Provision of information regarding the level of intrusion would also be of low value for the same or similar reasons and, therefore, APS does not support requiring these attributes as part of mandatory reporting.

Conversely, APS agrees that information regarding attack vectors could be more relevant, actionable information to be shared. To ensure the value of reporting, APS recommends that the Commission focus on the "What" and the "How" with regards to events. For example, the inclusion of information in the reporting that identifies the asset or asset type that was attacked and the vector that was used to attack it would provide valuable, actionable information because, relative to attack events, the methodology is more important than the technical details given the variances in infrastructure across the industry. Of additional value is information regarding the actions that other entities took to prevent or mitigate the effects or impacts of the Cyber Security Incident. For these reasons, APS does not support the inclusion of all attributes proposed by the Commission in the NOPR and urges the Commission to focus any reporting-related content requirements on information such as methodology, attack vector, asset/asset type, and response activities as this is information that other entities would find useful and actionable.

Finally, APS notes that this type of information is collected in the Form OE-417. Both the content and format of the reporting pursuant to Form OE-417 are conducive to effective communication, timely determinations regarding applicability, and the ability to take timely, effective response/preventative actions. APS respectfully urges the Commission to leverage the existing reporting mechanisms available such as the Form OE-417, which are proven, well-established mechanisms of sharing the information contemplated within the NOPR as discussed by the Commission therein.[6]

D. APS Supports Report Timing That Comports With The Timing Requirements Of Form OE-417.

If the Commission does decide to direct NERC to modify the CIP Standards to include a new mandatory reporting obligation, the timing for reporting on incidents that could, but didn’t, cause harm to the BES and/or facilitate subsequent efforts to harm the reliable operation of the BES 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. That being said, such reports should be timely enough to provide notification and awareness to NERC, the Commission, and other Responsible Entities such that entities can triage and take preventative measures, as possible and necessary. APS respectfully recommends aligning the timing of any mandatory reporting obligations with the timing dictated in Form OE-417. As discussed above, Form OE-

[6] NOPR at P10.

417 requires the reporting of cyber and/or physical incidents that could potentially impact electric power system adequacy or reliability within six (6) hours of such incidents. It then requires a final report within 72 hours of the incident. These time frames allow entities sufficient time to respond to an incident and understand its characteristics while providing such information timely. They further allow entities to supplement, amend, and/or modify their initial report as more information is known. This submission scheme provides NERC, the Commission, and Responsible Entities with the best of both worlds, i.e., an initial, timely report and a more comprehensive final report.

As discussed above, APS respectfully recommends that the Commission not direct NERC to develop an independent, redundant reporting obligation, but rather focus on requiring broader distribution of the Form OE-417 where such form has been utilized to report cyber and/or physical incidents that could potentially impact electric power system adequacy or reliability. Nonetheless, APS recommends that any timing requirements for the reporting proposed in the NOPR should be no sooner than six (6) hours following the identification of the incident to allow Responsible Entities the time necessary to focus on response and to gather salient facts for reporting.

E. APS Suggests Several Potential Alternatives To The Mandatory Reporting Requirements Proposed In The NOPR.

The Commission has identified that reliability coordinators, balancing authorities, some generating entities, and electric utilities are already required to report information regarding cyber and physical events with the potential to impact power system adequacy and reliability to the Department of Energy via Form OE-

417 and that such reporting is occurring. Hence, APS recommends that the Commission consider requiring Responsible Entities to distribute any Form OE-417 submitted to report a physical attack or cyber event that could potentially impact electric power system adequacy or reliability to the parties cited by the Commission in its NOPR, *i.e.*, E-ISAC and ICS-CERT. Leveraging this existing reporting obligation would not only ensure that the value and benefit to reliability provided outweighs administrative burdens, but will also allow for greater coordination and collaboration amongst the government and regulatory entities tracking such events as all of these entities will have received the same reports and, therefore, will be in possession of the same or similar data and information for review and analysis.

Additionally, because this information is already available to DOE, APS also recommends that NERC, the Commission, ICS-CERT, etc. leverage their inter-agency cooperation and data sharing processes to ensure that the reported data is shared. Placing the burden on Responsible Entities to submit the same or similar information to multiple agencies when those agencies can easily share such data inter-agency and, then, subjecting the Responsible Entities to a mandatory fine or penalty should it miss a particular entity on distribution is unjustified. For this reason, APS recommends the establishment of a minimum threshold of entities to which the entity must submit its report. For example, if the entity submits the report to the DOE and ICS-CERT, but fails to submit to the E-ISAC, such should not subject that entity to a mandatory penalty or non-compliance as that report has been timely submitted to a federal agency and is, therefore, available to other federal agencies, etc. through inter-agency sharing/cooperation.

Further, the issuance of a request for data or information pursuant to Section 1600 of the NERC ROP would not effectively address the reporting gap and current lack of awareness of cyber-related incidents; would not satisfy the goals of the proposed directive; would complicate data sharing; would create an independent, redundant reporting obligation to NERC or a regional entity; and would then subject the provision of such information to the E-ISAC and/or ICS-CERT to the confidentiality and data sharing processes set forth in Section 1500 of the ROP, delaying such sharing and distribution unnecessarily. Such process is not only multi-layered and inefficient, but creates a scenario under which Responsible Entities have redundant obligations to report, *e.g.*, via Section 1600 and Form OE-417, creating administrative burden for NERC, regional entities, and Responsible Entities unnecessarily.

Additionally, because the data submitted qualifies for confidentiality protections under Section 1500, it creates the need to address and incorporate into the data sharing process the requirements for sharing confidential information under Section 1500 of the NERC ROP. Thus, before NERC or a regional entity could share reported incidents to the E-ISAC or ICS-CERT, certain data sharing provisions would be required to be addressed. These include notifications to the submitting and any other impacted entity, which require monitoring and, potentially, response. It may also result in the inability of such entities to further share or distribute such information. Such 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.

For these reasons, APS respectfully asserts that a simple requirement to distribute any Form OE-417 submitted to DOE to report a physical or cyber incident that could potentially impact electric power system adequacy or reliability to the E-ISAC and ICS-CERT or simply relying upon the submission of such reports to DOE and, then, inter-agency sharing and cooperation easily satisfy the Commission's objectives as expressed in the NOPR.

Finally, APS agrees that the E-ISAC is well-positioned to clearly identify valuable information regarding Cyber Security Incidents, share such information with Responsible Entities, and help the industry understand and respond to what has been shared. However, their tools and processes are not optimized to support this function. For example, there is not, currently, a deadline by which information submitted to the E-ISAC must be triaged and distributed. Additionally, there is not an Application Programming Interface ("API") through which information can be easily and quickly submitted. If the E-ISAC instituted a user-friendly API through which incident reports could be submitted and distributed as well as a required time period for distribution of reports that they receive, it could act as a timely clearinghouse, performing the functions that are necessary to satisfy the Commission's objectives as set forth in the NOPR. Currently, by the time the E-ISAC reports information received to industry, the information is dated and of little use.

The Commission's current proposal does not address these issues, which would continue to hamper the timely awareness of existing and future cyber security threats and vulnerabilities even if the Commission's proposal is ultimately implemented. Hence, APS respectfully recommends that this issue provides yet another reason for the Commission to consider leveraging Form OE-417 and enhanced inter-agency cooperation and sharing instead of its proposal described in the NOPR.

F. APS Supports The Filing Of An Annual Report To The Commission Provided That Such Report Is Filed And Maintained Pursuant To Confidentiality Protections.

APS acknowledges that it is clearly within the Commission's authority to require that NERC submit an annual report; however, it remains concerned that – even in an anonymized, summary format, the report could be utilized by hackers to hone their attacks and techniques. For this reason, if the Commission does enact such a requirement, APS recommends that the report be filed and maintained as confidential. Such reports could then be made available to the industry through the Critical Energy/Electric Infrastructure Information ("CEII") request process.

III. CONCLUSION

For the foregoing reasons, APS respectfully requests that any subsequent action taken by the Commission in this proceeding be consistent with the comments set forth herein.

Respectfully submitted,

/s/ Kristie Cocco
Kristie Cocco
Director, Regulatory Affairs, NERC
Pinnacle West Capital Corporation
400 North 5th Street
Mail Station 8695
Phoenix, AZ 85004
(602) 250-4464
Kristie.cocco@aps.com

/s/Christina Bigelow
Christina Bigelow
Senior Attorney
Pinnacle West Capital Corporation
400 North 5th Street
Mail Station 8695
Phoenix, AZ 85004
(602) 250-2404
Christina.Bigelow@pinnaclewest.com

Dated: February 16, 2018

Document Content(s)

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 MICROSOFT CORPORATION

Pursuant to the Notice of Proposed Rulemaking issued by the Federal Energy Regulatory Commission ("FERC" or the "Commission") in the above-referenced proceeding,[1] Microsoft Corporation ("Microsoft") submits these comments regarding the Commission's proposed modifications to the Critical Infrastructure Protection ("CIP") reliability standards. Microsoft appreciates the Commission's interest in ensuring that there is sufficient awareness and understanding of threats that could undermine reliability. However, Microsoft is concerned that the proposal does not provide sufficient guidance as to how the modified CIP reliability standards would apply to entities that are registered with the North American Electric Reliability Corporation ("NERC") ("Registered Entities") and that use a commercial cloud service such as Microsoft's Azure and Azure Government services to operate cloud-based "BES Cyber Systems" (as that term is defined by the NERC). Importantly, Microsoft requests the Commission to confirm that cloud service providers that provide services to Registered Entities are not required to register with NERC based on their provision of those services, and that cloud service providers, as opposed to the Registered Entity to which services are provided, are not responsible for compliance with the CIP reliability standards. Microsoft believes that clarification on these issues is important to foster technical innovation that will improve the

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

economy, security, and reliability of the bulk electric system ("BES") in a manner that is consistent with NERC's risk-based approach to compliance monitoring and assessment.

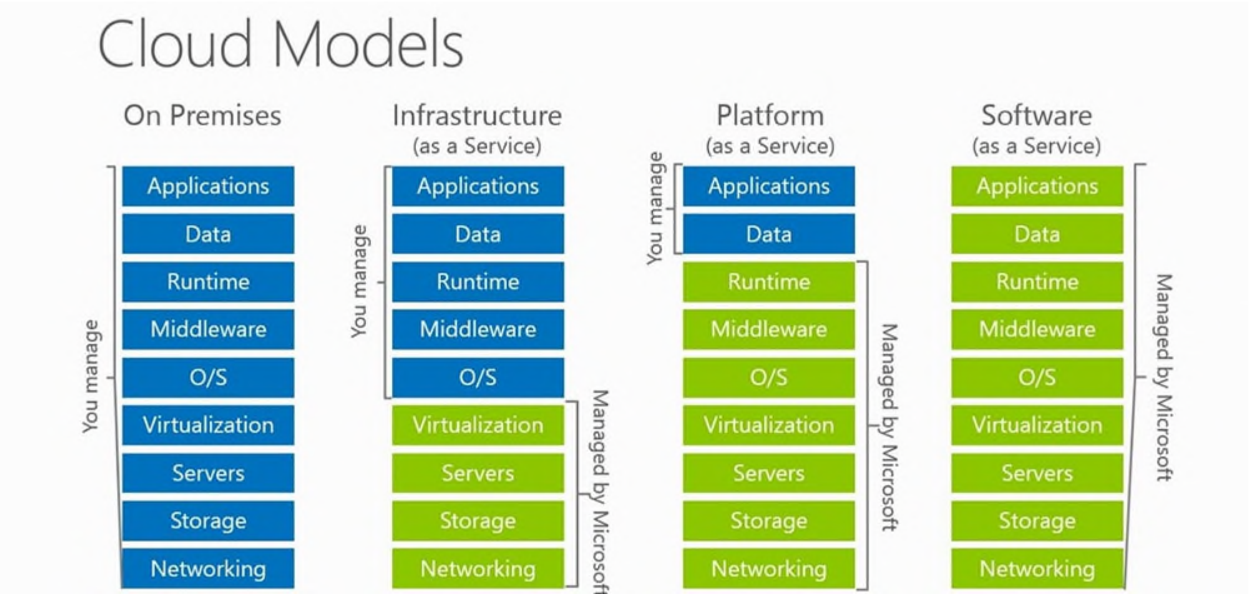
I. The cloud computing services that Microsoft provides to Registered Entities may be more secure than services from on-premises deployment.

Microsoft offers comprehensive cloud computing services, including servers, storage, databases, networking, software, analytics and more, that are available to Microsoft customers via a common, internet-based cloud infrastructure and platform.[2] One of the primary benefits of cloud computing is the concept of a shared, common infrastructure across numerous customers simultaneously leading to economies of scale. This concept is called "multi-tenancy."

Consistent with the NIST definition of cloud computing, tenants of the Microsoft cloud can choose from one of three cloud service models: Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Software as a Service ("SaaS"). Under the IaaS model, Microsoft offers servers, storage, networking and virtualization, and the customer manages all operating systems, software, applications and data stored in the cloud. Under the PaaS model, Microsoft manages the operating system and basic software in addition to services provided under the IaaS model, while the customer manages applications and data. Under the SaaS model, Microsoft manages the services and data at the application layer, but customers remain responsible for administering the services, including granting proper access rights to end users. Figure 1, below, provides a representation of the shared responsibility model in cloud computing and how it compares to traditional on-premises deployment.

[2] The National Institute of Standards and Technology ("NIST") defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or support provider interaction." U.S. Dept. of Commerce, Nat'l Institute of Standards and Technology, *The NIST Definition of Cloud Computing* (Sept. 2011) available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Figure 1: On Premises Management v. Cloud Service Models



A multi-tenant cloud platform implies that multiple customer applications and data are stored on the same physical hardware. Microsoft uses logical isolation techniques to separate cloud tenants and create an environment where customers can access and manage only their own cloud-based resources. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously enforcing controls designed to keep customers from accessing one another's data or applications.

Microsoft personnel have very limited access to customers' cloud-based resources, which is outlined in the contracts for services. Access to customer resources is only permitted for Microsoft to operate its commercial cloud services. When access is required, it is done so via just-in-time access using temporary credentials, and all actions by Microsoft personnel are logged and audited. Controls for the protection of customer secrets are audited on a regular basis as part of existing independent third-party audits. Customers also have several options for encrypting their data in the cloud, including keeping encryption keys in hardware security modules that are FIPS 140-2 Level 2 validated.

II. The Commission should confirm that cloud service providers do not need to register with NERC based solely on their provision of cloud services to Registered Entities.

Microsoft does not perform any BES functions via its cloud services that would subject it to registration under NERC's functional model. The only assets that Microsoft controls are the hardware and software that underlie the Microsoft cloud services offerings, which can be used by Registered Entities for a variety of purposes, including to run cloud-based BES Cyber Systems. Because Microsoft cannot control how its customers use the cloud services procured from Microsoft, and because cloud services are not regulated by FERC, Microsoft concludes that (i) cloud service providers are not required to register with NERC with respect to their ownership and operation of the cloud, and that, (ii) as a result, cloud service providers are not subject to the requirements set forth in the CIP reliability standards.

Unfortunately, commercial cloud customers who are Registered Entities that operate cloud-based BES Cyber Systems may be confused because there is currently no guidance from NERC regarding the use of commercial cloud services. Similarly, it is not clear to Registered Entities how to treat commercial cloud services under the CIP reliability standards. Registered Entities can use the Microsoft cloud to manage their BES Cyber Systems in a secure, efficient and cost-effective manner. Registered Entities using the Microsoft cloud own and remain in complete control of all their cloud-based systems, including any BES Cyber Systems. Although Registered Entities can engage Microsoft for help with preventing, detecting, and responding to threats, Microsoft does not own or control any BES Cyber Systems through the provision of its cloud services. Accordingly, Microsoft should not be subject to NERC registration or the requirements of the CIP reliability standards. In line with the shared responsibility concept in cloud computing, however, Microsoft will assist Registered Entities with their own NERC CIP compliance obligations for assets deployed to the cloud.

To the extent required by NERC and permitted under Microsoft's legal obligations and customer commitments, Microsoft will assist its Registered Entity customers in any required reporting requirements under the CIP reliability standards. However, it remains unclear if and to what extent Registered Entities that use cloud-based BES Cyber Systems require additional information from their cloud service providers to report BES Cyber Incidents or attempted incidents. Accordingly, as explained more fully below, the Commission should clarify the extent to which its proposed modifications to the CIP reliability standards will affect Registered Entities that own and operate cloud-based BES Cyber Systems. Microsoft suggests that prior to issuing a final rule in this proceeding, the Commission should convene a technical conference for industry stakeholders, including vendors, to discuss how NERC should implement the proposed modifications as well as potential impacts to Registered Entities and their cloud service providers.

III. The Commission should exempt cloud infrastructure from CIP direct reporting requirements.

To date, neither the Commission nor NERC has provided any clear guidance on the extent to which Registered Entities that use commercial cloud-based BES Cyber Systems must report incidents, or attempted incidents, relating to their use of cloud infrastructure. Registered Entities that use cloud services should be responsible for ensuring their own compliance with the reporting requirements set forth in the CIP reliability standards with respect to their management, configuration, and operation of their cloud-based BES Cyber Assets, rather than placing the onus on a commercial cloud service provider that operates a multi-tenant environment. Moreover, the

Commission should clarify what constitutes an "attempted" incident, especially with respect to a Registered Entity's cloud-based BES Cyber Systems.

As explained above, Microsoft uses logical isolation techniques to segregate each customer's applications and data from those of others. Pursuant to their contracts with Microsoft, electric utilities and other Registered Entities that use the cloud maintain complete control of their tenancies and cloud-based applications, including securing those tenancies and applications (*e.g.*, application firewalls and anti-malware software). Microsoft, as a provider of a commercial cloud services, (1) has very limited visibility into the tenancies of its customers, and (2) does not know if a customer is a Registered Entity or whether a customer that is a Registered Entity is operating a BES Cyber Systems within its tenancy.

When Microsoft becomes aware of a cyber incident affecting its cloud services, Microsoft reports relevant information regarding impacted customers in accordance with its contractual commitments and legal obligations. Microsoft does not – and does not have the necessary expertise to – determine whether any security incident impacted a specific portion (*e.g.*, the Electronic Security Perimeter ("ESP") or Electronic Access Control or Monitoring Systems ("EACMS")) of a Registered Entity's cloud-based BES Cyber Systems. Only the Registered Entity that owns and operates the BES Cyber Systems has sufficient visibility relating to the effects of cyber security incidents on its BES Cyber Systems. In addition, cloud service providers such as Microsoft are legally and contractually obligated to maintain confidentiality of their customers' information. Microsoft would therefore be unable to provide known accurate or meaningful information to NERC or the Commission relating to a successful or attempted cyber security incident relating to a Registered Entities cloud-based BES Cyber Systems.

Microsoft reports any cyber incidents that affect a customer directly to that customer and provides information and support to assist the customer in analyzing the business impacts of the cyber incidents. It is the responsibility of the customer – which is the Registered Entity – to report the incident to NERC, as may be required by laws or standards applicable to the customer. Microsoft believes that this approach for handling cyber incident reporting for each customer is preferable and consistent with the CIP reliability standards, since it permits Registered Entities to meet their own reporting requirements and assess the significance of any harmful effects of malware under the CIP reliability standards as they may be modified in this proceeding. It also ensures that NERC will receive only relevant information that is useful in making risk-based decisions on cybersecurity.

To better define the limits of Registered Entity's reporting requirements with respect to cloud-based BES Cyber Systems, Microsoft requests that the Commission clarify that the ESP and EACMS of Registered Entity's cloud-based BES Cyber Systems apply to the Registered Entity and not to a cloud service provider. As explained above, within the cloud, each tenant maintains independent control of its cloud-based resources. Also as explained above, to the extent that a cyber security incident occurs, the Registered Entity, as the customer, is in the best position to have sufficient information to report to the Commission. Accordingly, the Commission should clarify that when a Registered Entity uses commercial cloud services, (i) its ESP and EACMS do not extend beyond the Registered Entity's subscription within the cloud, and (ii) the appropriate reporting body is the Registered Entity and not the cloud service provider.

This clarification is necessary because Microsoft and other cloud services providers manage their cloud platforms for use by millions of customers, many of which are not involved in the NERC-regulated electric utility industry. Microsoft does not report security incidents to customers that are not impacted by security incidents; confidentiality requirements prevent Microsoft from disclosing such information. In addition, it would be unduly burdensome, and would not result in any improvements to reliability or security, to require Microsoft to train its global workforce on Cyber Security Incident reporting in each of several particular industry sectors, including the electric industry, since Microsoft neither controls nor manages any information regarding BES Cyber Systems that a Registered Entity (or any other customer) might operate in the cloud. While Microsoft could notify Registered Entities of incidents that may impact their data or tenancies, Microsoft employees would not be aware of or be able to identify specific types of BES Cyber Assets or potential impact on BES operations as a result of a Registered Entity's decision to operate a part of its services in the cloud.

Accordingly, Microsoft should not be required to report incidents to the Commission or NERC relating to data and resources controlled by and belonging to Microsoft's other tenants. Moreover, logical isolation of tenancies within the cloud help ensure that any breach of another tenant's cloud-based resources cannot affect a Registered Entity's cloud-based resources. Under NERC's risk-based approach to compliance monitoring, there is little to no value in requiring a cloud service provider to identify and disclose information that is unrelated to a Registered Entity's subscription in the cloud.

To the extent that the Commission or NERC wishes to implement a baseline level of security that Microsoft and other cloud service providers offer to Registered Entities, it would be appropriate for the Commission and NERC to recognize as effective one or more third-party certifications, such as those that Microsoft has earned for the security of its Azure and Azure Government offerings. Both Azure and Azure Government are audited extensively by independent third-party auditors. Azure has the broadest compliance coverage in the industry, including key independent certifications and attestations such as ISO 27001,[3] ISO 27017, ISO 27018, ISO 22301, ISO 20000-1, ISO 9001, Service Organization Controls ("SOC") 1/2/3, Payment Card Industry ("PCI") Data Security Standard ("DSS") Level 1,[4] HITRUST Alliance,[5] Cloud Security Alliance ("CSA") Security, Trust & Assurance Registry ("STAR") Certification,[6] CSA STAR Attestation,[7] and Federal Risk and Authorization Management Program ("FedRAMP") Moderate Provisional Authorization to Operate ("P-ATO") issued by the Joint Authorization Board ("JAB").[8] In terms of U.S. government focused compliance coverage, Azure Government has:

- FedRAMP High P-ATO issued by the JAB;
- Department of Defense ("DoD") – Defense Information Systems Agency – Security Requirements Guide – "Level 4 Provisional Authorizations";
- NIST Federal Information Processing Standard 140-2 "Level 2" certification for cryptographic module validation;
- Contractual amendments available to support FBI Criminal Justice Information Services and Internal Revenue Service IRS 1075 requirements;

[3] The ISO standards are developed and managed by the International Organization for Standardization ("ISO"). Based in Switzerland, ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies.
[4] PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.
[5] Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain.
[6] CSA is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.
[7] CSA STAR attestation is a collaboration between CSA and the American Institute of Certified Public Accountants ("AICPA") to provide guidelines for certified public accountants to conduct SOC 2 engagements using criteria from the AICPA and CSA.
[8] The General Services Administration manages FedRAMP as a government-wide program providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- Contractual amendment to support U.S. Department of State – Directorate of Defense Trade Controls – International Traffic in Arms Regulations requirements; and
- Support for NIST "Special Publication" 800-171 guidance for the protection of Controlled Unclassified Information.

Accordingly, resources that are uploaded to the Microsoft cloud are maintained safely and securely pursuant to numerous third-party, certified and internationally-recognized standards. In contrast, Registered Entities that operate their BES Cyber Systems on-site are not required to operate and maintain their hardware or software pursuant to these rigorous standards. Compliance with the requirements of these certifications and attestations helps ensure that resources operated on the Microsoft cloud are more secure than the on-site operations of a Registered Entity; and the Commission should make every effort that neither its rules nor NERC's reliability standards undermine the ability of Registered Entities to benefit from this heightened level of security.

Microsoft has sought guidance from NERC staff on best practices for Registered Entities that use the cloud to demonstrate compliance with CIP requirements. In discussions with NERC staff, the following independent third-party programs were identified as relevant and potentially useful to Registered Entities with cloud-based BES Cyber Assets:

- CSA STAR program;
- American Institute of Certified Public Accountants SOC 2 Type 2 attestation; and
- FedRAMP authorization.

Each of these certifications and attestations provides evidence of Microsoft's stringent compliance with industry leading cyber-security standards, which go above and beyond the security requirements established by NERC. To the extent that the Commission and NERC provide guidance to Registered Entities for adoption of cloud technology, they should accept these certifications on behalf of Registered Entities that operate cloud-based BES Cyber Systems as evidence of a cloud service provider's compliance with the NERC's risk-based compliance monitoring and assessment program, including as it relates to requirements under the CIP reliability standards.

IV. Conclusion

Based on the foregoing, Microsoft requests that the Commission confirm that cloud service providers are not required to register with NERC and, as a result, are not subject to the requirements set forth under the CIP reliability standards. In addition, to the extent that Microsoft must provide any information to the Commission, NERC, or a Registered Entity with cloud-based BES Cyber Systems, the Commission should clarify that Microsoft and other cloud service providers are not required to report any cyber incidents to any entity other than their customer. Rather, Microsoft recommends that the final rule make clear that cloud service providers are only required to comply with their contractual obligations to report incidents to customers. To the extent that NERC requires further assurances from Microsoft or other cloud service providers on behalf of their Registered Entity customers, NERC should rely on third-party certifications and attestations, such as those described herein.

Respectfully submitted,

/s/ Adam Wenner

Adam Wenner
A. Cory Lankford
Orrick, Herrington & Sutcliffe LLP
1152 15th Street, N.W.
Washington, DC
Tel: (202) 339-8400
awenner@orrick.com
clankford@orrick.com

Counsel for Microsoft Corporation

Dated: February 26, 2018

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Notice of Proposed Rulemaking	**)**	
Cyber Security Incident	**)**	**Docket No. 18-2-000**
Reporting Reliability Standards	**)**	

COMMENTS OF THE ENERGY SECTOR SECURITY CONSORTIUM, INC. (ENERGYSEC)

I. Introduction

The Energy Sector Security Consortium, Inc. (EnergySec) is a United States 501(c)(3) non-profit corporation formed to support energy sector organizations with the security of their critical technology infrastructures. Through our programs, we support collaborative initiatives and projects that help enhance the cybersecurity resiliency of these organizations.

Although our comments are informed by input from our members and broader community, EnergySec does not speak on behalf of our members or any other organization. These comments are attributable only to EnergySec.

II. COMMENTS

As an organization that has supported cybersecurity-related information sharing efforts for more than 15 years, we are generally in agreement with the Commission's goal of increasing the frequency and detail of incident reporting. However, we have serious concerns regarding aspects of the Commission's proposal, including the scope of incident reporting, the timing, and the content of reports. We also have comments and suggestions regarding alternative approaches to support increased reporting of cybersecurity incidents.

Commission concerns

The Commission's proposals are supported by stated concerns in the NOPR. The Commission states, "The current reporting threshold for Cyber Security Incidents, as set forth in Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning) together with the definition of Reportable Cyber Security Incident, may understate the true scope of cyber-related threats facing the Bulk-Power System"[1]. The Commission furthers states that it intends to require reporting of certain incidents, "before they have caused such harm or if they did not themselves cause any harm"[2], since, "unsuccessful attempts to compromise or disrupt a responsible entity's core activities are not subject to the current reporting requirements."[3] The Commission justifies modifying the reporting threshold by reference to a current requirement that, "mandates logging of detected successful login attempts, detected failed access attempts, and failed login attempts".

In the above comments, we believe the Commission errs in two ways. First, "compromise" as used in the definition of Reportable Cybersecurity Incident does not necessarily imply harm. We contend that an incident should be considered a "compromise" if an attacker has obtained the ability to disrupt, even if no disruption occurs. Second, the Commission equates failed access attempts and blocked network traffic with attempts to compromise, using such as a justification for expanded reporting of attempted attacks. However, the referenced requirement pertains to logging of events, an activity which is useful for analysis of potential compromises, but which is not directly comparable to mandatory incident reporting.

Although we share the Commission's concern that current reporting

[1] NOPR at ¶3

[2] NOPR at ¶1

[3] NOPR at ¶27

does not accurately portray the level of cyber incidents in the industry, we believe the reporting threshold is appropriate. As reflected further in our comments below, we believe that a clarified understanding of the current definition of Reportable Cybersecurity Incident can sufficiently address the Commission’s concerns. Specifically, we believe the current definition can be construed to include certain non-impactful incidents, as well as incidents affecting Electronic Security Perimeters (ESPs) and Electronic Access Control and Monitoring Systems (EACMS).

Scope of incidents that require reporting

Regarding the scope of the proposed reporting standards, we have several concerns. First, the Commission’s proposal is overly broad. The proposal would require reporting, “including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system.”[4] Such a determination would be highly subjective and could easily be construed to include systems and networks that are outside the scope of the Commission’s authority. The Commission also proposes to include “attempts to compromise.”[5] In its discussion, the Commission equates a failed login or access attempt with an attempt to compromise. However, most failed logins or access attempts are benign in nature. Also, the volume of such events is orders of magnitude larger than what would be an appropriate volume for mandatory reporting. While we agree that reporting of “near-miss” events could be useful and should be encouraged, we believe it would be counterproductive to attempt to mandate such reporting in a reliability standard.

The Commission further proposes to mandate reporting of incidents that “… attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).” We generally agree that successful attacks against ESPs and EACMS should be within the scope of reporting; we disagree with the proposal to include attempted compromise in the reporting

[4] NOPR at ¶2

[5] NOPR at ¶31

requirements. Determination 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. We note that the NERC Rules of Procedures require standards to be objectively measureable. Specifically, section 302 states, "Each performance Requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that Requirement."[6] The probable result of this directive would be requirements that cannot be objectively audited and, therefore, violate NERC's Commission approved Rules of Procedure.

With respect to the inclusion of EACMS in the scope of reporting, we suggest that monitoring-only systems be excluded from this requirement. Although compromise of monitoring systems could assist an attack, such a compromise would not directly permit access. Additionally, inclusion of such a requirement would discourage the deployment of certain modern approaches to monitoring, such as the use of MSSPs and other 3rd party services, including cloud based analysis, threat intelligence, and event aggregation services.

Recipient of reports

With respect to the designated recipients of mandatory incident reports, we have no objections to the proposal, but offer suggested modifications to provide flexibility to Registered Entities that may reduce the reporting burden of new requirements. The Commission proposes "to continue having the reports go to the Electricity Information Sharing and Analysis Center (E-ISAC) instead of the Commission, but we propose to require that reports also be sent to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and that NERC file an annual, public, and anonymized summary of the reports." We agree that the E-ISAC is an appropriate ultimate destination for all required incident reports, but suggest that entities should be explicitly allowed to channel such reporting through 3rd parties. Many electric utilities participate in

[6] NERC Rules of Procedure, Section 302, Item 3

information sharing groups and services in addition to their interactions with the E-ISAC. For example, some public power entities utilize the Multi-State Information Sharing and Analysis Center (MS-ISAC). Other utilities work closely with various state fusion centers. And others have close connections with local or regional Information Sharing and Analysis Organizations (ISAOs).

Allowing reporting to flow through 3rd parties would accomplish three important objectives. First, it would reduce or eliminate potential duplication of effort for organizations that utilize 3rd parties extensively in the incident response and analysis process. Second, it would encourage the further development of information sharing organizations beyond the ISAC that may be better positioned to serve specific entities. And third, it could allow for anonymity in reporting, thereby alleviating lingering concerns about sharing sensitive information with the E-ISAC.

Should the Commission determine that 3rd party reporting is appropriate and should be allowed, we suggest that the NERC should be directed to develop formal procedures for interacting with such 3rd parties to facilitate information flow and obtain certainty that the required incident reports are being received by the E-ISAC in a timely manner.

In its NOPR, the Commission states that its proposed modifications of the reporting requirements, "will enhance awareness for NERC, industry, the Commission, other federal and state entities, and interested stakeholders regarding existing or developing cyber security threats."[7] This statement clearly indicates that the scope of appropriate parties extends beyond just the E-ISAC, and supports our suggestion to allow 3rd party involvement in incident reporting.

Content of reports

The Commission proposes to require reports to include, "(1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to

[7] NOPR at ¶4

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."[8] While such information would be useful, we are concerned that including this as a requirement could be construed to require significant forensic and analysis efforts. Any such requirement must clearly identify the limits of any required forensic activity to ensure that undue burdens are not imposed.

Timing of Reporting

The Commission also proposes to require NERC to develop, "deadlines for filing a report once a compromise or disruption to reliable bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity". We agree that clear timelines should be part of any new incident reporting requirements. We also agree that the timelines should factor in the severity of the incident and the level of effort required to complete an investigation. We are concerned that short reporting deadlines may make thorough investigations impractical. We suggest that interim reporting at regular intervals be allowed for ongoing investigations.

Alternative approaches

"The Commission also seeks comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards."[9] We suggest that, in lieu of prescriptive new reporting requirements, the Commission could direct NERC to require entities to develop and implement an information sharing plan. 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. We believe that such an approach would encourage an increased flow of relevant cybersecurity information within the industry, support

[8] NOPR at ¶38

[9] NOPR at ¶36

innovative approaches, and encourage the growth of local, regional, and other ISAOs that augment the current capabilities of the E-ISAC and Registered Entities.

III. Conclusion

EnergySec appreciates the opportunity to submit comments in response to the NOPR.

Respectfully submitted,

Steven H. Parker
President
Energy Sector Security Consortium, Inc.
steve@energysec.org

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE
THE ISO/RTO COUNCIL

The ISO/RTO Council ("IRC") respectfully submits these comments in response to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR") for possible modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards regarding the improvement of mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System ("BES").[1]

The IRC generally supports FERC's proposed expansion of Cyber Security Incident reporting obligations, which will help to provide greater transparency of cybersecurity threats to industry. However, the IRC believes that the proposed requirement to report all "attempts to compromise" an Electronic Security Perimeter ("ESP") or associated Electronic Access Control or Monitoring Systems ("EACMS")[2] needs further clarification. The Independent System Operators ("ISOs") and Regional Transmission Organizations ("RTOs") observe tens of thousands of interactions with their ESPs each day, and determining with certainty which of these interactions was made

[1] *Cyber Security Incident Reporting Reliability Standards,* Notice of Proposed Rulemaking, 82 FR 61,499 (Dec. 28, 2017).

[2] NOPR at PP 30, 33.

with a nefarious motive, or which of them could have had some more serious consequence had they not been stopped at the ESP, would be nearly impossible. Conservative compliance policy could effectively require each ISO and RTO to report all such events, exponentially increasing the reporting burden and reducing the effectiveness of the reports due to their sheer volume.

The IRC therefore urges FERC to provide greater clarity in the reporting obligation by allowing industry to identify the specific events that would be considered "attempts to compromise" such that the reporting obligation would be invoked. This would ensure both that compliance with the reporting requirement is achievable and that the report provides meaningful information.

IDENTIFICATION OF FILING PARTY

The IRC is comprised of the following ISOs and RTOs: Alberta Electric System Operator ("AESO"); California Independent System Operator Corporation ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator ("IESO"); ISO New England Inc. ("ISO-NE"); Midcontinent Independent System Operator, Inc. ("MISO"); New York Independent System Operator, Inc. ("NYISO"); PJM Interconnection, L.L.C. ("PJM"); and Southwest Power Pool, Inc. ("SPP"). [3]

[3] The AESO and IESO are not FERC jurisdictional. Accordingly, AESO does not join these comments.

II. COMMENTS

A. ANY REPORTING STANDARD SHOULD INCLUDE CRITERIA THAT CAREFULLY DEFINE REPORTABLE INCIDENTS

In the NOPR, FERC proposes to direct the North American Electric Reliability Corporation ("NERC") to develop and submit modifications to the CIP Reliability Standards to improve the reporting of Cyber Security Incidents to include not only those incidents that actually impact an ESP or EACMS, but also unsuccessful attempts to compromise the ESP or EACMS.[4] The proposed development of a modified mandatory reporting requirement is intended to improve awareness of existing and future cyber security threats and potential vulnerabilities.[5]

In response to the Commission's request for comment on this proposal,[6] the IRC submits that a reporting standard developed by NERC must be: (1) clear and achievable; (2) sufficiently narrow to prevent inundating the Electricity Information Sharing and Analysis Center ("E-ISAC") or applicable entity with reports of attacks that present no or minimal risk of creating harm, thereby rendering reports meaningless; and (3) sufficiently broad to ensure the true scope of cyber-related threats are not underreported. The IRC believes the proposed modifications to the reporting requirements fall short of these objectives.

Without 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

[4] NOPR at PP 30, 33.

[5] *Id.* at P 2.

[6] *Id.* at P 35.

unachievable, and will likely result in inundating the E-ISAC with unhelpful reports. It is not always possible to determine whether an interaction with an ESP or EACMS that does not cause any harm was simply an innocent attempt to gather information or was the first stage of an attack that would have impacted the reliable operation of the BES but for the effectiveness of the ESP. Given the lack of clarity as to when an incident would qualify as an "attempt to compromise," responsible entities could insulate themselves from compliance risk only by reporting all interactions with the ESP or EACMS. But in the case of each of the ISOs and RTOs, this would require the reporting of *tens of thousands* of interactions with the ESP and EACMS every day. Reporting each of these events would impose an impossibly onerous burden on ISOs/RTOs and would inundate E-ISAC and other report recipients with unhelpful information.

Instead of a broad requirement to report "attempts to compromise" the ESP or EACMS, the IRC recommends that the Commission revise its proposal to direct NERC to develop a set of reporting criteria in the standard that would provide some credible indication that an observed interaction with the ESP/EACMS is a consequence of a malicious act and not merely an innocuous communication with an ESP/EACMS that would not have caused further harm had it not been stopped. These criteria could be based on the stage of deployment to which the attack has advanced,[7] or the importance of the systems targeted by the attack, or other factors. Examples of such criteria might include: (1) if discovered, persistent compromise and attempts to pivot to critical systems

[7] *See* discussion of various attack stages in "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case" (March 18, 2016) ("E-ISAC Report"), available at http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

that could be interpreted as facilitation efforts to harm reliable operation of the BES; (2) insider incident involving access to ESPs; (3) incidents involving ICS systems (such as ICCP network or server equipment); (4) incidents involving physical access that could involve BES Cyber Systems, and (5) incidents with progress along a kill chain to the Modify/Install step.[8] IRC recommends that this or similar criteria be clearly defined while at the same time allowing flexibility to accommodate the diversity of security approaches and network designs of responsible entities.

B. ADDING EACMS TO THE MANDATORY REPORTING REQUIREMENT WOULD BE BENEFICIAL

FERC proposes modifications to the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS. FERC proposes to establish a compromise, or an attempt to compromise, a responsible entity's ESP or associated EACMS - due to their close association with ESPs - as triggering a reportable Cyber Security Incident. FERC seeks comment on whether to exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold.[9]

The IRC believes 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. Information shared with the E-ISAC regarding attacks on these systems may provide useful data for analytics

[8] E-ISAC Report, supra n. 7.

[9] NOPR at PP 4, 30, 33, 36.

that would be beneficial for situational awareness and communication to the industry.

C. ALTERNATIVES TO MANDATORY REPORTING REQUIREMENTS

FERC seeks comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards. Specifically, FERC seeks 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.[10]

The IRC submits that a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure would not be a preferable alternative. The purpose of the reporting requirements is to share valuable information about cybersecurity risks with industry. If the information were provided only pursuant to a request, then the requests (and responses) would need to be continual to ensure that all necessary information is provided, and a standing requirement to report would achieve the same result without the administrative burden of handling multiple data requests.

The IRC submits that another alternative FERC could consider is allowing entities to comply with the reporting requirements by participating in the Cyber Risk Information Sharing program. This program allows responsible entities to automatically report information to the E-ISAC for analysis against classified information held by E-ISAC and has demonstrated value to industry through enriched analytic products. In addition, the E-ISAC is developing automated information sharing capabilities using

[10] NOPR at P 36.

ThreatConnect and STIX/TAXII. 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.

D. A STANDARD FORM FOR REPORTS SHOULD BE REQUIRED

FERC proposes to direct that NERC modify the CIP Reliability Standards to specify the required content in a Cyber Security Incident report. FERC proposes that the minimum set of attributes to be reported should include: (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident. FERC seeks comment on this proposal and, more generally, on the appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities.[11]

The IRC believes that it will be beneficial for responsible entities to report indicators of compromise that are detected in potential cyberattacks against their systems in a standard form. Indicators of compromise may be the only information that a responsible entity has. Indicators of compromise are a common element that responsible entities can provide with certainty. Cyberattacks are detected at various stages and levels of consequence, so this information should be considered optional in an incident report. Other information regarding the potential impact, attack vector, and level of intrusion

[11] NOPR at PP 38, 40.

may require several weeks of forensic investigation and may require relying upon third parties to be determined. As a result, any incident reporting form should be considered a point in time record that may change over time.

E. THE TIMING OF A REPORT SHOULD BE DETERMINED ACCORDING TO THE SCALE AND SCOPE OF THE INVESTIGATION

FERC states that, while CIP-008-5 currently requires an initial notification of a Reportable Cyber Security Incident to E-ISAC within one hour of the determination that the incident is reportable, it does not require a specific timeframe for completing the full report. FERC seeks comment on the appropriate timing for Cyber Security Incident reporting to better ensure timely sharing of information and thereby enhance situational awareness.[12]

The timeframe for completing a full report depends on the scale and scope of the investigation. This will vary for each cyberattack. FERC should consider requiring that reports be updated at a certain frequency until the full report is complete. A 90-day report update requirement would be reasonable until the investigation can be completed and the full report submitted.

F. DETAILED REPORTS SHOULD ONLY BE REQUIRED TO BE PROVIDED TO E-ISAC

FERC proposes that reports submitted under the enhanced mandatory reporting requirements would be provided to E-ISAC, similar to the current reporting scheme, as well as to the Industrial Control System Cyber Emergency Response Team ("ICS-

[12] NOPR at PP 41, 43.

CERT"). The detailed incident reporting would not be submitted to FERC.[13] FERC also proposes to direct NERC to file publicly an annual report reflecting the Cyber Security Incidents reported to NERC during the previous year. Specifically, FERC proposes to direct NERC to file annually an *anonymized* report providing an aggregated summary of the reported information.[14]

Reporting of incidents and attempts should be done with a single destination and common format. Requiring reporting to multiple destinations imposes additional burden on responsible entities that should instead be handled with information sharing between destinations (*i.e.* E-ISAC and ICS-CERT in this case). Detailed incident reports should only be required to be provided to E-ISAC, and it should be noted that details regarding entities should not be available to entities other than E-ISAC.

The IRC supports having the E-ISAC develop and file an annual anonymized report to FERC for reported incidents. This will provide FERC with situational awareness and will help to ensure that NERC and other compliance organizations do not have attributable information on such incidents.

[13] NOPR at P 40.

[14] *Id.* at PP 2, 42, 43.

III. CONCLUSION

The IRC requests that the Commission consider these comments on the NOPR.

Respectfully submitted,

/s/ *Anna McKenna*
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ *Carl Patka*
Robert E. Fernandez, General Counsel
Raymond Stalter,
Director of Regulatory Affairs
Carl Patka, Assistant General Counsel
Christopher R. Sharp, Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
csharp@nyiso.com

/s/ *Margoth R. Caley*
Raymond W. Hepper
Vice President, General Counsel, and Secretary
Theodore J. Paradise
Assistant General Counsel, Operations and Planning
Margoth R. Caley
Senior Regulatory Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ *Craig Glazer*
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
Suite 600
1200 G Street, N.W.
Washington, D.C. 20005
202-423-4743
Craig.Glazer@pjm.com
James.Burlew@pjm.com

/s/ *Stephen G. Kozey*
Stephen G. Kozey
Senior Vice President
Joseph G. Gardner
Vice President & Chief Compliance Officer
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
stevekozey@misoenergy.org

/s/ *Nathan Bigbee*
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
Nathan.bigbee@ercot.com

/s/ Tam Wagner
Tam Wagner
Senior Manager, Regulatory Affairs
Maia Chase
Senior Regulatory Analyst
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto Ontario M5H1T1
Canada
tam.wagner@ieso.ca
maia.chase@ieso.ca

/s/ Paul Suskie
Paul Suskie
Executive Vice President, Regulatory Policy
& General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

Dated: February 26, 2018

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Holyoke, Massachusetts this 26th day of February, 2018.

/s/ Julie Horgan
Julie Horgan
eTariff Coordinator
ISO New England Inc.
One Sullivan Road
Holyoke, MA 01040
(413) 540-4683

Document Content(s)

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 EVERSOURCE ENERGY SERVICE COMPANY

Eversource Energy subsidiary, Eversource Energy Service Company,[1] ("Eversource Energy") hereby submits comments in response to the Notice of Proposed Rulemaking issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") on December 21, 2017, in the above-referenced docket.[2]

Eversource Energy believes the NOPR'S expansion of the scope of reportable Cyber Security Incidents to "attempted" intrusions into Bulk Electric System ("BES") Cyber Systems and related security perimeters will create ambiguity in compliance responsibilities and may lead to excessive reporting of incidents that will not make the electric grid more secure from cybersecurity incidents. Further, expanding the amount of required information to be reported and increasing the number of recipients of the reports will create undue administrative burdens; and may undermine ongoing voluntary information sharing activities that already work effectively to increase electric industry awareness of cybersecurity threats. As a result, Eversource Energy does not support the proposed modifications.

[1] Eversource Energy Service Company is the Registered Entity responsible for compliance with all North American Electric Reliability Corporation ("NERC") reliability standards applicable to Eversource Energy affiliates.

[2] *Cyber Security Incident Reporting Reliability Standards*, 161 FERC ¶ 61,291 (2017), Notice of Proposed Rulemaking, 82 FR 61499 (Dec. 28, 2017) ("NOPR").

I. COMMENTS

Eversource Energy owns and operates electricity transmission and distribution systems within the three-state region of Connecticut, New Hampshire, and Massachusetts. Eversource Energy serves a highly diverse geographic area spanning 13,220 square miles and safely and reliably operates over 21,200 miles of transmission and distribution infrastructure.

Eversource Energy is committed to maintaining the reliability of the BES. In addition to the mandatory cyber intrusion reporting requirements under CIP-008-5, Eversource Energy also participates in voluntary arrangements for reporting cyber intrusion events to the electric sector to share information appropriately, and develop appropriate responses to mitigate risks to the BES.

Under the currently effective Critical Infrastructure Protection ("CIP") Reliability Standard CIP-008-5, responsible entities are required to send an initial notification within one hour from the determination of a Reportable Cyber Security Incident to the Electricity Information Sharing and Analysis Center ("ES-ISAC").[3] The current definition of reportable events in CIP-008-5, a Reportable Cyber Security Incident, requires mandatory incident reporting of only those incidents that have "compromised or disrupted one or more reliability tasks."

The Commission proposes to direct NERC to modify the Reliability Standard CIP-008-5 to increase the scope of Cyber Security Incident reporting due to concerns that the current

[3] Requirement R1 and Table R1 Cybersecurity Incident Response Plan Specifications

reporting threshold "may not reflect the true scope of cyber-related threats facing the BES."[4] The Commission proposes to expand the threshold of reportable events to include ***attempted*** incidents that "***might*** facilitate subsequent efforts to harm the reliable operation of the bulk electric system (emphasis added)." The proposed new reporting threshold will add incidents that compromise Electronic Access Control or Monitoring Systems ("EACMS") and attempts to compromise or attempt to compromise a responsible entity's Electronic Security Perimeter ("ESP") or associated EACMS to the existing threshold.

In addition, the NOPR proposes to broaden the number of entities that must receive Cyber Security Incident reports. The current standard requires responsible entities to report only to the Electric Sector Information Sharing and Analysis Center ("ES-ISAC") in coordination with the U.S. Department of Energy ("DOE"). The NOPR would require responsible entities to also report Cyber Security Incidents to the U.S. Department of Homeland ("DHS") Security Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"). Finally, the NOPR would (1) expand the required reporting information;[5] (2) mandate specific reporting timeframes;[6] and (3) require NERC to annually file an anonymized public summary of the reports.[7]

The following are Eversource Energy's concerns with the NOPR:

[4] NOPR at P 24.

[5] The proposed expanded reporting content includes: (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident.

[6] Under the current CIP-008-5 standard, a responsible entity only is required to submit an initial notification of a reportable event to ES-ISAC, but the standard does not require a specific timeframe for completing the full report. The NOPR directs the development of specific incident report timeframes based on the actual or potential threat to reliability. NOPR at P 41.

[7] NOPR at P 2, 4.

Ambiguity of Reportable Incidents - The proposed changes to the definition of Reportable Cybersecurity Incident will make compliance by responsible entities extremely difficult and will not improve the overall effectiveness of the electric industry's responses to cybersecurity threats. This is because of the ambiguity in determining which attempted incidents could have harmed the BES when such intrusions were unsuccessful. Making such an assessment would require Eversource Energy to speculate about the hypothetical consequences of every unsuccessful attempt to compromise a responsible entity's cyber assets. Alternatively, because the term "attempted compromise" in the proposed Cyber Security Incident Report contents is ambiguous, the modifications proposed in the NOPR may lead to overreporting of information "just to be safe" resulting in dissemination of unhelpful, and potentially overly-burdensome amounts of information to process by enforcement bodies, threat analysis entities, and the industry. In sum, the meaning of "attempted compromise" is too ambiguous to provide adequate notice of a responsible entity's compliance obligations under the proposal and needs to be clearly defined.

Change in Intent of Reporting Requirements- Adding attempts to compromise the BES to the existing mandatory CIP-008-5 reporting requirements will alter the intent of this reporting standard from information reporting to the ES-ISAC in support of information sharing and aiding system restoration to an alternative threat intelligence focus, which already is currently performed through existing voluntary arrangements with government and industry. The existing mandatory incident reporting requirements in CIP-008-5 is focused on notifying the ES-ISAC of cybersecurity incidents and disruptions caused by actual compromises to BES Cyber Systems. If the Commission is seeking to change this purpose to gathering threat and potential threat intelligence information more comprehensively, the reliability need should be carefully balanced with the burden introduced by the new NERC standard requirements.

Impact on Effective Voluntary Information Sharing Programs - The proposed modifications introduce new technical and administrative challenges that will likely impact responsible entities' ability to participate in existing voluntary threat information sharing programs. Further, the voluntary cyber-threat information sharing arrangements Eversource Energy and others engage in to heighten risk awareness could be undermined by the added burdens of meeting the new proposed standards.

Eversource Energy currently coordinates closely with the ES-ISAC, DOE, DHS, and NERC's Critical Infrastructure Protection Committee ("CIPC") to detect, analyze, and share threat and vulnerability information through voluntary partnerships. Eversource Energy information technology subject matter experts share significant amounts of data with the government, including detected unusual or suspicious activity. Government analysts work with Eversource Energy and the ES-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. These voluntary programs have proven their value because the protocols in place already have been successful in enhancing threat analysis.

Eversource Energy is concerned that modifying the CIP Standards to mandate such voluntary information sharing will introduce new redundant and significant administrative burdens, which may harm these important voluntary security partnerships. If the standards proposed in the NOPR are adopted, responsible entities will be incentivized to prioritize mandated compliance reporting information included in the NERC standard which may be less useful, leaving fewer resources available to engage in voluntary, and potentially more valuable information sharing.

Additional Burdens- As described above, the meaning of an attempted compromise is currently undefined and may impose significant burdens on responsible entities to identify such attempts. Determining whether incidents are actual attempted compromises would require further analysis to determine whether the cyber intrusion was a deliberate attempt to compromise the BES. The analysis needed to determine whether attempted intrusions are actual attempts to compromise the BES is likely to be time and resource intensive. More work needs to be done to determine the technical feasibility of identifying and analyzing potential attempted compromises before NERC can begin drafting modifications to the CIP standards. To balance these concerns while addressing the Commission's reliability and awareness concerns, Eversource Energy recommends that the Commission continue to require initial incident reporting and additional incident analysis ***only*** to the ES-ISAC of ***actual*** cybersecurity compromises of the BES. Additional reporting of incidents involving the ESP and associated EACMS should be done on a voluntary basis in coordination with ES-ISAC, ICS-CERT, and CIPC. Alternatively, the Commission should consider expanding the categories identified in the NERC Events Analysis Program to include compromises of the ESP and associated EACMS, as a workable alternative to the CIP-008 NOPR proposal.

II. CONCLUSION

Eversource Energy appreciates the opportunity to submit comments in response to the NOPR. As discussed above, the Commission should limit mandatory reporting to the ES-ISAC and provide for a voluntary process, similar to NERC's Event Analysis Program, to further analyze actual compromises of the ESP and associated EACMS. Eversource Energy does not support the modifications proposed by the Commission in the NOPR because they may harm existing threat information sharing partnerships, create redundant and ambiguous reporting requirements and introduce new technical and administrative challenges that require further study before implementation. Accordingly, Eversource Energy believes it would be prudent for the Commission to convene a technical conference to address these concerns before directing NERC to modify the existing CIP-008 standards.

Respectfully submitted,

__/s/ Mary Ellen Paravalos__
Mary Ellen Paravalos
Vice President, ISO, Siting and Compliance
Eversource Energy Service Company
247 Station Drive
Westwood, MA 02090
(781) 441-8738
maryellen.paravalos@eversource.com

__/s/ Andrew S. Katz
Andrew S Katz
Senior Counsel
Eversource Energy Service Company
901 F Street, N.W. Suite 602
Washington, D.C. 20004
(202) 508-0903
andrew.katz@eversource.com

Dated: February 26, 2018

Document Content(s)

CENTER FOR SECURITY POLICY

Frank J. Gaffney, Jr., President & CEO

25 February 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18–2–000, Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, Commissioner Powelson, and Commissioner Glick:

After serving in the Reagan administration in various positions, including acting as the Assistant Secretary of Defense for International Security Policy, I founded the Center for Security Policy – a not-for-profit, non-partisan educational corporation which strives to provide timely, informed analyses and recommendations concerning critical foreign and defense policy challenges.

Among the most critical of those challenges are the various, looming threats to America's electric grid. Consequently, from the time of the Commission on the Electromagnetic Pulse (EMP) Threat's first report to Congress in 2004 to the present day, the Center – like many other leaders in the national security arena – have been warning that the grid's lack of resilience poses a potentially existential danger to our country.

As you know, this vulnerability can be exploited by enemies using a variety of techniques including physical sabotage, electromagnetic attack, or cyberattack. Given that the very survival of our nation depends upon the protection of grid assets against these forms of attack, there is great public interest in doing so.

Ample evidence exists in the public domain pointing to the rapidly increasing risk of malware present in information technology (IT) and operational technology (OT) associated with electric grid infrastructure, posing a grave and immediate danger to the American people who depend on this infrastructure for daily life.

As Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency testified before the U.S. House Select Intelligence Committee on November 20, 2014, he made clear that "foreign cyber actors are probing America's critical infrastructure networks and in some cases have gained access to those control systems." One month later, cyber security vendor Cylance published its “Operation Cleaver” report, demonstrating that Iran-based hackers had compromised at least one U.S. electric generation company. One year later, on December 23, 2015, the world witnessed 225,000 electricity customers lose power after a sophisticated cyberattack struck the Ukrainian grid, leveraging a family of malware that enabled attackers to use stolen user credentials to take over grid operators’ control stations, delete data on hard drives, remotely open circuit breakers at more than 120 electric substations, schedule disconnects for Uninterruptible Power Systems (UPS), and damage substation equipment necessary for power restoration. A year following that, in December 2016, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) publicly reported on this Russian military/civilian intelligence-developed malware tool, called “BlackEnergy,” in its Joint Analysis Report (JAR) titled “GRIZZLY STEPPE – Russian Malicious Cyber Activity.” This JAR was proof of the real and direct danger to electric grids by malware, since BlackEnergy was previously identified by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the Department of Homeland Security (DHS) as being present in America’s energy sector.

Incredibly, even with just the publicly available evidence mentioned above, under current North American Electric Reliability Corporation (“NERC”) standards, electric utilities do not generally consider the detection of malware to be a “Reportable Cyber Security Incident.” Even worse, NERC standards do not require the removal of malware, but rather only its “mitigation,” without any requirement for such mitigation to take place in a timely manner.

As pointed out by the Foundation for Resilient Societies in its *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), “notable malware requirement gaps in the NERC cybersecurity standards include:

1. No required reporting of malware infections, both inside and outside the Electronic Security Perimeter.
2. No specific timeframes for malware removal, both inside and outside the Electronic Security Perimeter.
3. Equipment necessary for reliability operation of the Bulk Power System may nonetheless be exempted from malware requirements because loss of this equipment would not impact reliability within 15 minutes. Examples include backup generation, uninterruptible power supplies (UPS), and heating, ventilation, and air n, conditioning (HVAC) systems.
4. All communication networks outside of the Electronic Security Perimeter are exempted from malware requirements, even when these networks are necessary for reliable grid operation. The exemption of communication networks from malware requirements conflicts with a specific mandate in Section 215 of the Federal Power Act to secure “communication networks” from “cybersecurity incidents.”
5. All Low-Impact assets, including those that are part of the Bulk Power System, are exempted from malware requirements.
6. No required malware detection, reporting, mitigation, or removal for IT systems, even when these systems are interconnected with OT systems and the public internet.”

Knowing that adversaries of the United States have already proven capable of blacking out electric grids via cyberattack and since these enemies are likely to increase malicious cyber activities inside of North American based electric grid infrastructure prior to other types of attack (such as EMP or physical sabotage), we consider it necessary that the Federal Energy Regulatory Commission ("FERC" or "the Commission") order NERC to set an enhanced standard for malware detection, reporting, mitigation, and removal ("Malware Standard"). When determining the technical elements of a Malware Standard, FERC should order NERC to include – at a minimum – the fourteen elements listed by The Foundation for Resilient Societies in the aforementioned Docket No. AD17-9.

FERC has the authority under Section 215(d)(5) of the Federal Power Act to order a proposed reliability standard to address the yawning gaps in the current NERC cybersecurity policy. Such action would shore up both grid security and national security writ large since it could help facilitate multi-direction information sharing between U.S. intelligence agencies, cybersecurity vendors, and electric utility companies and also help both the Executive and Legislative branches of government conduct proper strategic planning to deal with adversaries targeting the nation's electric grid.

Given the proven reality that malware has been introduced into grid-related IT and OT by the nation's adversaries and the incredible costs associated with prolonged blackouts that could be caused by a cyberattack, we believe that FERC must act most expeditiously to order NERC to create an enhanced standard for malware detection and reporting and that NERC should ensure that both malware mitigation and removal also take place posthaste.

Sincerely,

Frank J. Gaffney
President and CEO

cc: Hon. Rick Perry, Secretary of Energy

Document Content(s)

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 LARGE PUBLIC POWER COUNCIL

I. INTRODUCTION AND EXECUTIVE SUMMARY

These comments are filed by the Large Public Power Council ("LPPC") in response to the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking, issued in this docket on December 21, 2017.[1] LPPC appreciates FERC's interest in developing additional information regarding attempts to compromise Electronic Security Perimeters ("ESPs") and associated Electronic Access Control or Monitoring Systems ("EACMS"), but believes that the proposed directive may yield a substantial quantity of unhelpful information and confusing analyses, while needlessly burdening Registered Entities. For that reason, if FERC proceeds with a directive, LPPC recommends that the Commission take these measures:

- Before finalizing any directive, FERC should direct the North American Electric Reliability Corporation ("NERC") and industry to work together to establish a sensible threshold for determining which attempts to compromise ESPs and EACMS warrant reporting.
- The process of determining what information may productively be the focus of data collection might begin with a FERC-sponsored technical conference aimed at

[1] *Coordination of Protection Systems for Performance During Faults and Specific Training for Personnel Reliability Standard*, 161 FERC ¶ 61,159 (2017) ("NOPR").

defining the definitional threshold for any new reporting requirement and the range of assets to which it applies.

- FERC should provide NERC with the flexibility to employ a data request issued under Section 1600 of its Rules of Procedure ("ROP"), rather than a mandatory Reliability Standard.

A. LPPC

LPPC is an association of the 26 largest state-owned and municipal utilities in the nation and represents the larger, asset-owning members of the public power sector.[2] LPPC members are also members of the American Public Power Associations ("APPA") and own approximately 90% of the transmission assets owned by non-federal public power entities. LPPC members are located throughout the nation, both within and outside RTO boundaries, and they are subject to the Commission's electric reliability regulations and requirements as set forth in Federal Power Act Section 215.

B. The NOPR

The Commission proposes to direct NERC to revise the Critical Infrastructure Protection ("CIP") Reliability Standards to broaden the scope of mandatory reporting under the standards to include "Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS."[3] The Commission further seeks comment on potential

[2] LPPC's members are: Austin Energy, Chelan County Public Utility District No. 1, Clark Public Utilities, Colorado Springs Utilities, CPS Energy (San Antonio), ElectriCities of North Carolina, Grand River Dam Authority, Grant County Public Utility District, IID Energy (Imperial Irrigation District), JEA (Jacksonville, FL), Long Island Power Authority, Los Angeles Department of Water and Power, Lower Colorado River Authority, MEAG Power Nebraska Public Power District, New York Power Authority, Omaha Public Power District, Orlando Utilities Commission, Platte River Power Authority, Puerto Rico Electric Power Authority, Sacramento Municipal Utility District, Salt River Project, Santee Cooper, Seattle City Light, Snohomish County Public Utility District No. 1, and Tacoma Public Utilities.

[3] NOPR at P 4. The currently-effective CIP standards provide that responsible entities must report a Cyber Security Incident only if it has compromised or disrupted one or more reliability tasks of a functional entity. *See* definition of

alternatives to modifying the mandatory CIP reporting requirements, including whether a NERC request for data under Section 1600 of NERC's Rules of Procedure may effectively address the reporting gap the Commission has identified.[4]

The Commission has also proposed to direct NERC to modify the CIP Reliability Standards to specify certain required information to be contained in Cyber Security Incident reports submitted by responsible entities, and to direct NERC to establish a deadline for filing such reports once a compromise or disruption to the Bulk Electric System ("BES"), or attempted compromise or disruption, is identified by a responsible entity.[5]

II. COMMENTS

1. If FERC proceeds, it should be mindful of ongoing information sharing programs, and the potential for a counter-productive effort.

In comments filed contemporaneously, Edison Electric Institute ("EEI") catalogues ongoing efforts aimed at eliciting and processing information related to BES threats and vulnerabilities that is currently being shared through voluntary partnerships and close coordination between responsible entities and the Electricity Information Sharing and Analysis Center ("E-ISAC"), the Department of Energy ("DOE"), and the Department of Homeland Security ("DHS").[6] LPPC agrees with EEI that a new requirement holds the potential to adversely affect the electric subsector's participation in these existing, voluntary industry and government partnerships, and may be counterproductive to the overall goal of sharing timely and actionable threat information. The concerns are threefold: (1) there will be a focus on the compliance burden of new requirements rather than security, with limited intelligence value; (2)

"Reportable Cyber Security Incident," NERC Glossary of Terms Used in the NERC Reliability Standards, *available at* http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[4] NOPR at P 36.

[5] *Id.*, PP 37-42.

[6] *See* Comments of EEI, Docket No. RM18-2 (filed Feb. 26, 2018).

the potential for collection of a great deal of information that is not actionable, potentially obscuring useful information; and (3) diversion of resources from voluntary efforts to share actionable information to compliance management with rigid requirement.

The industry currently coordinates closely with the E-ISAC, DOE, DHS, and the DOE National Laboratories on a variety of programs designed to detect, analyze, and share threat and vulnerability information through voluntary partnerships. Industry executives and their subject matter experts work directly with these entities and, indeed, do report attempted compromises when it is thought that shared information may be of value. Through these partnerships, the expertise and innovation of both industry and government is harnessed to improve threat and vulnerability detection, analysis, and sharing capabilities.[7]

With this as background, there is good reason to be concerned that a rigid mandate may have the effect of requiring responsible entities to shift their resources from efforts to share threat information voluntarily for purposes of security in order to focus on new and broadened compliance activities and reporting requirements. Ongoing and emerging efforts have worked best when they focus on the collection and dissemination of actionable information, while the collection of raw unfiltered data regarding unsuccessful efforts to breach systems may result in a cloud of unusable information. Moreover, a new mandatory requirement may be at odds with the aim of streamlining regulation (the Paperwork Reduction Act). Whatever action FERC takes here, accordingly, must be done with an eye toward causing as little disruption to existing information sharing programs as possible. As discussed below, LPPC believes this may best be

[7] Among the programs in which public power has been directly engaged showing substantial promise is the E-ISAC "Industry Augmentation Program," providing for direct participation of utility employees in E-ISAC operations, simultaneously facilitating industry familiarity with the E-ISAC and encouraging voluntary communication. See: https://www.publicpower.org/periodical/article/nypa-srp-cyber-experts-get-window-how-e-isac-handles-data.

achieved if FERC facilitates a dialogue with NERC and the industry that would help shape any information sharing requirement.

2. Before finalizing any directive, FERC should enable NERC and the industry to work together to establish a sensible threshold for determining which attempts to compromise ESPs and EACMS warrant reporting.

LPPC supports the request made by NERC in comments filed today to work with industry stakeholders to develop "a common threshold" for defining reportable "attempts to compromise:" that will enable NERC and the industry to focus on useful information, without overburdening responsive entities.[8] NERC further indicates that, given the flexibility to appropriately focus its data collection efforts, it would fine tune the focus on EACMS, recognizing that the risk associated with compromise of these devices varies considerably.

A reporting standard that is overly broad in scope could lead to the collection of an overwhelming amount of information, much of which may prove to yield little actionable information, while burdening responsible entities and potentially obscuring more valuable information. Accordingly, LPPC supports NERC's request for needed flexibility in defining the threshold reporting definitions. In addition, LPPC agrees with NERC's request for flexibility to determine the appropriate timeframe within which entities must submit to NERC their full reports regarding Cyber Security Incidents and attempts to compromise. These timelines will very likely affect how this information is used, ranging from early indication of potential attacks to analysis of trends over time.

[8] *See* Comments of NERC, Docket No. RM18-2 (filed Feb. 26, 2018).

3. This process of determining what information may appropriately be the focus of data collection may begin with a FERC-sponsored technical conference.

The Commission, NERC and the industry have productively used technical conferences in order to work toward consensus regarding the state of reliability and the merit of various proposals, including standards and compliance reform. Technical conferences were employed beneficially in discussing the nature and scope of NERC's initially proposed standards, in addressing a host of issues regarding the coordination of FERC's and NERC's respective responsibilities at a critical time in NERC's development, and in addressing the reform of NERC's compliance and monitoring programs.[9]

Here, 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. The focus of such a conference should be on what information already is being shared and made available currently through voluntary partnerships among responsible entities and various Federal government agencies, and through other channels, as well as how best to fashion a data request to target the collection of information from industry that will add the most value with respect to existing or developing cyber security threats.

4. LPPC Supports the Use of Data Requests through the NERC Rules of Procedure Section 1600 Process, rather than a Reliability Standard.

As an alternative to establishing a broad reporting requirement as part of the NERC Reliability Standards, LPPC supports a more flexible approach to collection of actionable

[9] *See, e.g., Mandatory Reliability Standards for the Bulk-Power System*, Notice of Technical Conference, Docket No. RM06-16 (issued May 31, 2006) (establishing a July 6, 2006 technical conference to consider NERC's proposed Reliability Standards, FERC Staff's Preliminary Assessment of those standards, and related issues); *Mandatory Reliability Standards for the Bulk-Power System*, Notice of Technical Conference, Docket No. RM06-16 (issued Aug. 19, 2010) (establishing a Sept. 23, 2010 technical conference to consider NERC's proposed frequency response-related Reliability Standards).

information through the data request process outlined in NERC ROP Section 1600. In its comments, NERC notes that this data collection process establishes an efficient and mandatory avenue for NERC to collect information from the industry. NERC also provides the assurance – critical to LPPC – that it would work with the industry in shaping the associated data requests.

As noted by NERC, the data request approach offers flexibility that the standards development process does not. As explained by NERC in its comments, the NERC ROP Section 1600 process allows for stakeholder input and FERC staff review of any data request proposed by NERC. Like Reliability Standards, compliance with a NERC data request is mandatory for applicable entities, while the data request procedures specified under ROP Section 1600 also provide a more efficient process to update or revise a data request as needed to respond to rapidly-changing security threats. This flexibility is important, and makes the data request process in NERC ROP Section 1600 a more suitable avenue to gather this information versus data collection through a Reliability Standard.

Further, it seems appropriate to remove the data collection process from the enforcement process associated with mandatory Reliability Standards. Responses to data requests are required, to be sure, but the compliance and sanctions process associated with mandatory standards is a poor fit for the collaborative information sharing process that LPPC believes FERC, NERC and the industry share the goal of promoting.

III. CONCLUSION

LPPC requests that the Commission consider the comments discussed above, as it contemplates the cyber security incident reporting proposals advanced in this docket.

Respectfully submitted,

/s/ Jonathan D. Schneider

Jonathan D. Schneider
Jonathan P. Trotta
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

Counsel to the
Large Public Power Council

Dated: February 26, 2018

Document Content(s)

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. <u>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.</u>

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

Document Content(s)

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 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)

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 AMERICAN PUBLIC POWER ASSOCIATION, ELECTRICITY CONSUMERS RESOURCE COUNCIL, AND TRANSMISSION ACCESS POLICY STUDY GROUP

The American Public Power Association ("APPA"), the Electricity Consumers Resource Council ("ELCON"), and the Transmission Access Policy Study Group ("TAPS") submit these comments on the Commission's December 21, 2017 Notice of Proposed Rulemaking.[1] The Commission's NOPR proposes to direct the North American Electric Reliability Corporation ("NERC") to develop a modification to its reliability standards to increase the scope of mandatory reporting requirements for cyber security incidents.

Instead of issuing the proposed directive, the Commission should consider whether tools other than a new or revised reliability standard could better achieve the goal of improving awareness of existing and future cyber security threats and potential vulnerabilities. Alternatively, if the Commission nevertheless directs the development of a new or revised standard, the Commission should give NERC flexibility to define appropriate reporting thresholds for actual and attempted cyber security incidents. Additionally (and regardless of whether the Commission directs NERC to develop a standard or instead adopts an alternative approach), the Commission should explicitly

[1] *Cyber Security Incident Reporting Reliability Standards*, 82 Fed. Reg. 61,499 (proposed Dec. 28, 2017), 161 FERC ¶ 61,291 (2017) ("NOPR").

state that it is not directing changes to the existing reporting requirements for low impact systems, and that NERC should implement any directive in a way that does not change the obligations for low impact systems.

I. INTERESTS OF APPA, ELCON, AND TAPS

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities account for 15% of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 49 million people in every state except Hawaii. Approximately 261 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout the United States. Many ELCON members also operate behind-the-meter generation and are NERC registered entities, and ELCON has actively participated in NERC's stakeholder and standards development processes. Reliable electricity supply is essential to its members' operations.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[2] TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are

[2] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

users of the Bulk Power System and are highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards.

Communications regarding these proceedings should be directed to:

For APPA
John E. McCaffrey, Regulatory Counsel
Jack Cashin, Director of Policy Analysis & Reliability Standards
American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
Email: jmccaffrey@publicpower.org
jcashin@publicpower.org

For TAPS
Cynthia S. Bogorad
Latif M. Nurani
Spiegel & McDiarmid LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
Email: cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

For ELCON
John P. Hughes
President & CEO
Electricity Consumers Resource Council
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390
Email: jhughes@elcon.org

John Twitty
Executive Director
Transmission Access Policy Study Group
PO Box 14364
Springfield, MO 65814
(417) 838-8576
Email: jtwitty@tapsgroup.org

II. COMMENTS

A. Modifying mandatory standards is not necessarily the best tool to achieve the goal of improving awareness of cyber security threats and potential vulnerabilities.

The NOPR explains that its proposed directive is intended "to improve awareness of existing and future cyber security threats and potential vulnerabilities."[3] That is an appropriate objective, but directing new or revised mandatory reliability standards is not

[3] NOPR, P 24.

the only tool that NERC and the Commission have for achieving that reliability objective. Mandatory standards, by their nature, cannot easily adapt to dynamic problems like cyber security threats. NERC's comments filed today in this proceeding recognize that alternate approaches, other than mandatory standards, should be used to achieve the goals the Commission seeks to achieve through the proposed directive.[4] Edison Electric Institute's comments, also filed today, describe several partnerships that are in place between registered entities and the federal government that help identify and improve awareness about cyber security threats and vulnerabilities. Importantly, these partnerships provide security tools that go beyond the potential mitigation of reliability standards.

Thus, particularly in the constantly evolving area of cyber security, which operates against the backdrop of rapidly changing technology, the Commission should consider and utilize the most flexible tools to achieve its reliability goals without imposing undue burden on registered entities.

B. If the Commission nevertheless issues a directive for a new or modified reliability standard, it should give NERC flexibility to define appropriate reporting thresholds for actual and attempted cyber security incidents.

The NOPR proposes to direct NERC to develop a revised reliability standard that would "include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP [Electronic Security Perimeter] or associated EACMS [Electronic Access Control and Monitoring System]."[5] If a Final Rule in this proceeding includes a directive to develop a new or revised standard, the

[4] NERC points to its existing authority under Section 1600 of its Rules of Procedure to collect data about cyber security incidents and vulnerabilities as preferable to a reliability standard.

[5] NOPR, P 30.

Commission should explicitly give NERC the flexibility to define appropriate reporting thresholds for attempted cyber security incidents.

As proposed, the NOPR's directive is potentially overbroad and could result in unduly burdensome reporting requirements that *reduce* awareness of significant cyber threats. Utilities experience near constant attempts to probe their firewalls to detect vulnerabilities. Requiring registered entities to report every attempted probe, even if the attempt is not a credible threat, could result in most utilities submitting multiple reports every day. Such a reporting obligation would be unduly burdensome on registered entities. Moreover, excessive reporting of non-credible attempts to compromise an EACMS would overwhelm the reports of credible attempts, thus making it more difficult to identify real cyber security threats and potential vulnerabilities.

The Commission should avoid such a result. If the Commission decides to direct a new or revised reliability standard, it should not include the proposed generic threshold of reporting *any* incidents that compromise or attempt to compromise an ESP or EACMS. Instead, it should give NERC sufficient flexibility to define appropriate reporting thresholds for attempted compromises of an ESP or EACMS so that the resulting standard is better able to advance its purpose of improving awareness of cyber security threats and potential vulnerabilities.

C. In any event, the Commission should clarify that it is not directing changes to the existing reporting requirements for low impact systems.

The NOPR appropriately focuses on medium and high impact BES cyber systems. The NOPR begins its discussion of the cyber security incident reporting threshold by discussing the existing reporting requirement in CIP-008-5, a standard that applies only to medium and high impact systems. And the NOPR's proposed directive—to require reporting of incidents that compromise or attempt to compromise an ESP or EACMS—necessarily refer only to medium and high impact systems, because ESPs and EACMS are terms that do not apply to low impact systems.[6] Commission Staff confirmed at the December 21, 2017 Open Meeting that the NOPR's focus on ESPs and EACMS "limits the proposal to high- and medium-impact BES Cyber Systems," and that the NOPR is "not touching on 'low' at this point."[7]

The NOPR's exclusion of low impact systems from the proposed expanded reporting requirements is appropriate. CIP-003-6 already requires owners and operators of low impact systems to identify Reportable Cyber Security Incidents and notify the ES-ISAC of them.[8] Consistent with the risk-based approach of the CIP standards, the reporting obligations for low impact systems allows for more flexibility than the reporting obligations for medium and high impact systems.[9] The Commission approved the existing incident reporting requirements in CIP-003-6 as providing appropriate security controls for low impact systems.[10] Expanding the reporting obligation for low impact systems would be unduly burdensome and not commensurate with the lesser risk that those systems pose to BES reliability. Additionally, given that there are many more

[6] *See* Revised Critical Infrastructure Protection Reliability Standards, Order No. 822, 81 Fed. Reg. 4177 (Jan. 26, 2016), 154 FERC ¶ 61,037, P 75 (2016) ("Order No. 822") *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016) ("We decline to adopt the recommendations . . . to modify the standards to utilize the concept of Electronic Security Perimeters for low impact systems.").

[7] Transcript of Commission Open Meeting at 26:14-17 (Dec. 21, 2017), https://www.ferc.gov/CalendarFiles/20180104102157-transcript.pdf.

[8] NERC, Reliability Standard CIP-003-6, Attachment 1, Section 4.2.

[9] Specifically, CIP-003-6 does not have the one-hour time limit for initial notifications of Reportable Cyber Security Incidents that is in CIP-008-5.

[10] Order No. 822, P 2.

low impact systems than medium and high impact systems, expanding the reporting obligation for low impact system increases the risk of creating excessive reporting full of "noise" that would make it harder to identify real threats. Thus, by excluding low impact systems, the NOPR correctly focuses on the most significant security threats associated with ensuring reliability.

If the Commission proceeds to issue a directive in this proceeding—whether it be a directive to develop a standard or a directive to use another tool to achieve the same goal—it should make plain that the directive is not intended to include low impact systems. While the NOPR indicates that it excludes low impact systems, the Final Rule should say so explicitly. Doing so would avoid potential confusion that could arise in implementing the directive.[11] Thus the Commission should clarify, if it does issue a directive, that it is not directing changes to the existing reporting requirements for low impact systems, and that NERC should implement the directive in a way that does not change the obligations for low impact systems.

CONCLUSION

For the reasons discussed above:

- The Commission should consider approaches other than directing a new or modified reliability standard to achieve the objective of improving awareness of cyber security threats and vulnerabilities;

[11] For example, the defined terms Cyber Security Incident and Reportable Cyber Security Incident are used in both CIP-003-6 for low impact systems and CIP-008-5 for medium and high impact systems.

- Alternatively, if a directive is issued, the Commission should give NERC flexibility to define appropriate reporting thresholds for attempted cyber security incidents; and
- In any case, the Commission should explicitly clarify in the Final Rule that it is not directing changes to the existing reporting requirements for low impact systems.

Respectfully submitted,

/s/ Cynthia S. Bogorad
Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000

Transmission Access Policy Study Group

John E. McCaffrey, Regulatory Counsel
Jack Cashin, Director of Policy Analysis
& Reliability Standards
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

American Public Power Association

John P. Hughes, President & CEO
ELECTRICITY CONSUMERS RESOURCE
COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390

Electricity Consumers Resource Council

February 26, 2018

Document Content(s)

Preston Le Roy Schleinkofer
President, Civil Defense Virginia
210-559-8625
preston@CivilDefenceVA.org

February 25, 2018

Chairman Kevin J. McIntyre
Commissioner Neil Chatterjee
Commissioner Cheryl A. LaFleur
Commissioner Robert F. Powelson
Commissioner Richard Glick
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Comments submitted in FERC Docket RM18–2–000
Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner Chatterjee, Commissioner LaFleur, and Commissioner Powelson, and Commissioner Glick:

I am a private citizen and the founder and president of the 501(c)(3) tax-exempt organization Civil Defense Virginia (CDVA). I have taken it upon myself for the past five years to learn about various threats to our country, more specifically the electrical power infrastructure. What I have learned is alarming; so alarming that I was motivated to found our organization to help prepare our communities for just such a catastrophe as the potential loss of our electrical power infrastructure for prolonged periods of time.

I am a retired federal law enforcement officer with over 27 years of service in the field and at headquarters in Washington, D.C. I am also a retired Sergeant First Class (E-7) with over 22 years of Active, Reserve and National Guard experience, the last 12 years of which was in a Nuclear, Biological, Chemical Defense Company supporting the now decommissioned 49th Armored Division, Texas Army National Guard. I believe that my experience and training has given me a unique outlook and the ability to see threats that others may not see. I see huge threats to our electrical power infrastructure.

Threats:

I see a variety of threats that mostly could be mitigated if we had the proper federal guidance and ability to enforce and penalize for non-compliance the many companies that make up our electrical infrastructure. I am a small government guy, but from my studies of the issue I am appalled at how unwilling and unresponsive the electrical power industry seems to be over these issues of grid hardening and reporting.

The major threats I see are man-made (*cyber attacks, physical attacks and electromagnetic pulse attacks*) and naturally occurring (*coronel mass ejection (CME), also known as space weather*) events that could very possibly endanger the lives of large portions of the US population. Some might say that these are low probability threats, which they are, but they are real and all have affected electrical power supply to some community or another in the past few decades. Maybe not all of them in the United States, but they have occurred, which is reason enough to take these threats seriously and protect against them. To think that "it couldn't happen here, in America" is naive and is not supported by real research and resent verbalized or insinuated threats by state and non-state actors.

Today is the most dangerous time in my adult life with the threats of war or attack by terrorists, Iran, North Korea, China and Russia, all of whom have the ability to attack our electrical infrastructure in one or more of the ways above. I and my organization would like to see these threats mitigated in the most expeditious way possible to ensure our national security and maintain continuity of community throughout our nation.

It appears to me, again, from my research and understanding of the issues and the lack of progress we have seen over the past 20 years, at least since the first warnings of the 2008 EMP Commission Report, the electrical power industry has seriously dropped the ball. It also seems that they have made attempts to downplay the seriousness of the need to harden our grid and used their influence on Capital Hill to stymie any attempt to provide your Commission authority to impose stricter rules and regulations and to enforce anything you would have them do.

The power grid is the most important component of our national infrastructure, without which none of the others could operate. And to think that they are resisting efforts to protect this system is just wrong. One would think that they would be the first to offer up ideas to protect their investments and income, but that doesn't seem to be the case.

We would urge you to require NERC to promulgate strict cyber-security standards and reporting requirements. In addition to these, we would suggest adding reporting on physical attacks as well. It is the duty of the federal government to protect America from all enemies and threats to our safety and security. If NERC is not required to report incidents of cyber attack, our national security will continue to be at risk through an industry not wanting to be regulated and unprepared for such attacks.

Respectfully submitted by:

Preston Le Roy Schleinkofer

File FERC RM18-2-000 Comments.PRN cannot be converted to PDF.

Document Content(s)

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting	**)**	**Docket No. RM18-2-000**
Reliability Standards	**)**	**Docket No. AD17-9-000**

COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES

Submitted to FERC on February 26, 2018

As initiator of this proceeding, by means of our Petition for Rulemaking filed with the Commission on January 13, 2017,[1] Resilient Societies appreciates the opportunity to comment on the subsequent Notice of Proposed Rulemaking (or "NOPR"), entitled "Cyber Security Incident Reporting Reliability Standards" and proposed by the Federal Energy Regulatory Commission ("FERC" or the "Commission") on December 21, 2017 in FERC Docket No. RM18-2-000.[2]

Background on Foundation for Resilient Societies

The Foundation for Resilient Societies, Inc. (or "Resilient Societies") is a 501(c)(3) non-profit organization engaged in scientific research and education to protect technologically-advanced societies from infrequently occurring natural and man-made disasters. With recognized policy and technical expertise in the use of federal and state regulations to protect electric grids from cyberattack, physical attack, solar storms, and electromagnetic pulse, our group is regularly asked to appear before official government bodies and industry forums. We have testified before the FERC, the Senate National Security and Defence Committee of the Canadian Parliament, and the U.S. House Committee on Oversight and Government Reform. We have deep expertise in the risks of long-term blackout and potential regulatory solutions, having made over two dozen filings in the reliability dockets at FERC and the Nuclear Regulatory Commission (NRC). Media sources such as the *Wall Street Journal, The Economist, Politico, USA*

[1] Petition for Rulemaking to require an enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System, 82 FR 9034-9035 (2017).
[2] 161 FERC ¶ 61,291, 82 FR 61499-61505 (2017).

Today, Reuters, NBC, and Fox News rely on our knowledge of critical infrastructure threats and cost-effective protections.

Summary of Cybersecurity Threats to the U.S. Electric Grid

In the 21st century, nations use threats against the infrastructure of other nations as instruments of power and as a means to deter attacks against their own country. Because electric grids are the keystone infrastructure, upon which all other infrastructures depend, electric grids are primary targets. Cyberattack is a preferred means of infrastructure attack, because it can be executed remotely, with minimal deployment of humans at physical risk. Because fewer resources are needed to execute a cyberattack, as compared to attack with conventional forces, it is an asymmetric and growing threat.

In November 2014, in testimony before the U.S. Congress, then-NSA Director Admiral Michael Rogers admitted that multiple foreign powers have the ability to take down the U.S. electric grid.[3] In February 2017, the Defense Science Board concluded that "limited U.S. efforts to defend U.S. information systems" make it impossible in the foreseeable future "to deny highly capable actors the ability to conduct catastrophic cyber attacks on the United States." In February 2018, the Office of the Secretary of Defense stated in its Nuclear Posture Review that the United States should posture its nuclear capabilities to hedge against non-nuclear strategic threats, including cyber aggression.[4] With weak cybersecurity protections for the U.S. electric grid, America is now forced to threaten first use of nuclear weapons as a deterrent to attack.

Gaps in Current NERC Cybersecurity Standards

We respectfully observe that hundreds of pages of cybersecurity standards proposed by NERC and approved by FERC have not been effective in mitigating strategic cyberattack threats, according to the head of the National Security Agency and the Defense Science Board. Why?

[3] Crawford, Jamie. "The U.S. government thinks China could take down the power grid," CNN. (November 21, 2014). Available at: https://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/index.html

[4] Office of the Secretary of Defense. "Nuclear Posture Review" Report. (February 2018). p. 38. Available at: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

Because NERC and its managers have incentives to set reliability standards that minimize compliance costs for the electric utilities. Representatives of electric utilities make up a super-majority of NERC membership and dominate its key governing bodies. Too often in the past, FERC Commissioners have acquiesced when NERC has proposed weak cybersecurity standards. Moreover, FERC has repeatedly recertified NERC as the designated "Electric Reliability Organization (ERO)." The electric industry is, de facto, the principal self-regulated industry in the United States. [5]

Gaps in NERC's cybersecurity standards are both pervasive and difficult for those outside the electric utility industry to ascertain. For example, so-called "low-impact" facilities are exempted from standards, even though attacks on high-impact facilities can be executed using low-impact facilities as the entry points. Furthermore, a simultaneous attack on several low-impact facilities can have a greater impact than a single attack on a "high-impact" facility. As another example, only a small fraction of the computer systems of electric utilities are covered under NERC's cybersecurity standards—those systems that control high voltage operations of the "bulk electric system": generation plants, switching substations, and control rooms. However, the business computer systems of electric utilities – used for accounting, personnel management, email, web browsing and the like – are connected to the public internet and therefore accessible to cyberattack teams around the world. Many U.S. electric utilities have electronically linked their operational systems to their business systems, thereby extending cyberattack vulnerabilities to computers that control the flow of power to homes and businesses.

[5] See also the comments submitted by Isologic, LLC in this Docket, prepared by the former chief scientist at the National Security Agency, George R. Cotter, a national expert on vulnerabilities of electric grids globally. Mr. Cotter asserts: "CIP Standards have simply failed to protect the Bulk Electric System and therefore the Distribution System, and therefore the infrastructures, institutions, and citizens nearly totally dependent upon the National Grid. Since 2012, Russia has conducted operations against the Grid, performed reconnaissance, collecting intelligence, and developing systematic attack systems…." The Isologic comments observe "The complete absence of an integrated Grid-wide capability to detect Attacks aimed at disabling or capturing a variety of local, regional or national targets represents a vulnerability of staggering proportions. How do Cyber Command and State National Guards respond?...FERC should require development and institutionalization of a nation-wide Situational Awareness structure; if the FPA [Federal Power Act] is a hindrance, Congress can amend the act." Isologic explains: "What is feasible is that a cybersecurity infrastructure across electric utilities (including Distribution assets) be put in place, a reasonable situational awareness program be established nation-wide, and realistic security standards and procedures be developed and enforced." For specific cybersecurity vulnerabilities and regulatory gaps, see the full Isologic comments filed in Docket RM18-2-000 on Feb. 6, 2018.

Occasionally, a gap in the NERC cybersecurity standards is obvious even to lay people and this self-regulatory organization will admit a problem. Such is the case with the current NERC standard for cybersecurity incident reporting. After zero cybersecurity incidents were reported for all of 2015, Resilient Societies urged the NERC Board of Trustees to address "materially misleading statements in regard to the number of reportable cybersecurity incidents" in their annual *State of Reliability* report.[6] While the NERC Trustees did slightly modify wording in their reports, NERC still allowed zero cybersecurity incidents to be reported in the subsequent year, 2016. During the same period, 2015 and 2016, the Defense Science Board, using information on electric grid cyberattacks that have gone unreported by utilities, concluded that grid cyber vulnerabilities are so severe they cannot be effectively defended against "in the near- to mid-term." [7]

In our experience from six years of observation of NERC standard-setting, when FERC proposes a remedy for a gap in reliability standards, NERC can often find a way to exempt significant numbers of electric utilities from taking protective action, even if an "improved" reliability standard is set.[8] The current proposal to require cybersecurity incident reporting only for compromise, or attempted compromise, of so-called "Electronic Security Perimeters" (ESP) and "Electronic Access Control or Monitoring Systems" (EACMS) is no exception. The FERC-proposed reporting threshold would give the NERC Standard Drafting Team wide latitude to craft ways that cybersecurity incidents need not be "reportable." Moreover, this threshold would clearly exempt electric utilities from reporting one of the greatest cybersecurity threats they face — insertion of malware into their business systems. When malware is present in business systems, it can then be used by cyber-attackers as a jumping-off point for attacks into operational systems, as the successful 2015 cyberattacks against utilities in Ukraine conclusively

[6] See Appendix 1 of this comment, containing the text of the May 12, 2016 Resilient Societies letter to the NERC Board of Trustees.

[7] The NERC "State of Reliability Report" with 2017 reported cybersecurity incidents will not be released until summer of 2018, but we expect the number of incidents for this past year to once again understate the true threat.

[8] For example, see Order No. 802, Physical Security Reliability Standard, 149 FERC ¶ 61,140 (Nov. 20, 2014), para. 91, 92 (NERC recommended exclusion of generators, accepted in FERC Order); para. 93 (NOPR excludes generators from physical security requirements); para. 99. As another example, under NERC Standard TPL-007-1, "Transmission System Planned Performance for Geomagnetic Disturbance Events," every transmission substation in the U.S. is effectively exempted from hardware protection by imprudent setting of the Benchmark GMD Event, combined with a high level of assumed transformer withstand to Geomagnetically Induced Currents.

showed. Malware infecting business systems can lay dormant, not even "attempting to compromise" Electronic Security Perimeters and their firewalls protecting operational systems.

Without care by the FERC Commissioners, the new standard developed in response to the December 21st FERC NOPR could minimize and delay reporting of cybersecurity incidents. Without care by the FERC Commissioners, fragmentary and incomplete cyber incident reporting will inappropriately diminish incentives for malware detection and removal. With minimal incident reporting, utilities will have less incentive for Red Team field testing and other "best practices" cyber-threat mitigation programs.

In our comments for this rulemaking, we cannot overemphasize this fundamental observation—the modifications proposed by FERC for mandatory cyber incident reporting will not require reporting of malware that is capable of causing widespread grid blackouts. As a result, the American public will remain at risk, unless the final ruling by FERC has substantial changes as compared to the December 21st Notice of Proposed Rulemaking (NOPR).

Based on six years of experience in FERC rulemaking for reliability standards to protect against high-impact events, we observe the final orders of the Commission generally conform closely to the requirements in the preceding NOPR. Comments from public stakeholders may be given *pro forma* consideration in the final ruling, but will often be placed aside in favor of the "solution" apparently negotiated between FERC and NERC. [9] Should the Commission once again decide to follow this path, we have this concern: *after NERC sets a new standard for cybersecurity incident reporting, and FERC approves the standard, there will still be minimal public reporting of cybersecurity incidents. Potential attackers will most often avoid breaching Electronic Security Perimeters until a full-scale attack is underway. The government, and the public, will lack a true picture of cybersecurity risks for the electric grid and this will prevent the societal consensus necessary for real protection to be implemented.*

[9] Based on a report that is now several years old, it is our understanding that FERC and NERC have a longstanding practice of holding quarterly, non-public meetings to discuss, *inter alia*, the status of reliability standards, including standards in development. Minutes of these quarterly meetings are withheld from public release by FERC. Such meetings give the impression of impropriety, especially when FERC-approved standards minimize compliance burdens but do not effectively protect the public against blackouts. We respectfully ask that the Commission open any regularly scheduled meetings with NERC to other public stakeholders and promptly release for public accessibility the minutes of all prior closed NERC-FERC meetings.

Report of the Defense Science Board

In February 2017, the Defense Science Board completed a two-year study on cyberattack deterrence, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence." In its report, the Board recognized that HAVEX and BlackEnergy malware have been discovered at U.S. electric utilities and concluded:[10]

> Although accelerating improvements to cyber defenses and resilience is vital to strengthen the U.S. posture and provide an essential foundation for deterrence by cost imposition, it will not be possible (for the foreseeable future) to deny highly capable actors the ability to conduct catastrophic cyber attacks on the United States. This is primarily because the limited U.S. efforts to defend U.S. information systems to date are unlikely to accelerate (in the near- to mid-term at least) to the point where they can offset the combination of major powers' technical wherewithal, vast supply of resources (including a supporting intelligence apparatus), and the ability to influence supply chains and exploit vulnerabilities at scale.
>
> However, the United States could – and must – aim to deny North Korea and Iran the ability to undertake catastrophic attacks on U.S. critical infrastructure via cyber, just as the United States aims to deny them the ability to attack with nuclear weapons.

During the same two years of the Defense Science Board study (2015 and 2016), U.S. electric utilities reported zero cybersecurity incidents under the standards of the North American Electric Reliability Corporation (NERC).

Report of the Council of Economic Advisers

The Council of Economic Advisers concluded in its February 16, 2018 report, "The Cost of Malicious Cyber Activity to the U.S. Economy," that the private sector has incentives to underinvest in cybersecurity, while cyberattack costs to the public could be enormous:[11]

> Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. *Failure to account for these negative*

[10] Defense Science Board Task Force on Cyber Deterrence, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence." Report. (February 2017) Available at: https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[11] The Council of Economic Advisers, Executive Office of the President. "The Cost of Malicious Cyber Activity to the U.S. Economy." Report. February 2018. p. 1, 41, 42. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

> *externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.*
>
> A cyberattack on the electrical grid could have large-scale economic impacts as infrastructure damages, loss in output, delayed production, spoiled inventory, and loss of wages all decrease productivity and earnings for the duration of the blackout.
>
> In addition to the economic impacts of a large power outage, there are health and safety concerns. Power outages impacting heating and cooling systems, at home health systems, refrigeration, and slower emergency response will all increase the rate of illnesses and death in the impacted areas. People will suffer from heat related conditions (such as heat stroke) and hypothermia, spoiled food, and difficulty of emergency responders to communicate with those impacted. In addition, riots, looting, and arson attacks as well as lack of lighting and overstretched police will increase crimes and decrease safety. (Emphasis added.)

Congress recognized the divergence between private sector economic incentives and the need for public protection when it mandated that FERC approve reliability standards “in the public interest.” However, under NERC standard-setting practices that minimize compliance burdens, utility investment in cybersecurity has been minimized to the detriment of the public interest.

New Information on Cyberattacks Targeting Electric Utilities

New information has come to light since the February 2017 closure of the comment period for Docket AD17-9-000 for the original rulemaking. Multiple credible sources report cyberattacks recently targeting electric utilities.

A June 12, 2017 article in USA Today, “Malware discovered that could threaten electrical grid,” revealed a new variant of malware, “Industroyer”:[12]

> A new malware variant capable of knocking out networks that run power grids around the globe has been discovered by a computer security company studying an attack on the Ukrainian power grid.
>
> The malicious code is capable of directly controlling electricity substation switches and circuit breakers and could potentially be used to turn off power distribution or to

[12] Weise, Elizabeth. “Malware discovered that could threaten electrical grid,” USA Today. (June 12, 2017). Available at: https://www.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998/

> physically damage equipment used in the electricity distribution grid, researchers at ESET wrote in a paper posted Monday.
>
> Two things stand out about the malware, dubbed "Industroyer" by the researchers — it's an order of magnitude easier to use than previous programs and it wasn't actually deployed to do any real damage, meaning whoever's behind the December attack might simply have been testing the waters.

A September 6, 2017 article in *Wired* magazine, "Hackers Gain Direct Access to U.S. Power Grid Controls," states that Symantec has detected a campaign of cyberattacks and intrusions at U.S. power firms:[13]

> Symantec on Wednesday revealed a new campaign of attacks by a group it is calling Dragonfly 2.0, which it says targeted dozens of energy companies in the spring and summer of this year. In more than 20 cases, Symantec says the hackers successfully gained access to the target companies' networks. And at a handful of US power firms and at least one company in Turkey—none of which Symantec will name—their forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.
>
> Those attacks were designed to harvest credentials from victims and gain remote access to their machines. And in the most successful of those cases, including several instances in the US and one in Turkey, the attackers penetrated deep enough to screenshot the actual control panels for their targets' grid operations—what Symantec believes was a final step in positioning themselves to sabotage those systems at will.

A September 7, 2017 article in *USA Today*, "Intrusion - but no attack - on U.S. energy grid is a warning, says former NSA official," gave additional details on compromised operational systems:[14]

> Over the last nine months, dozens of U.S. power companies were compromised by an organized hacking group to the extent that some of them could have sabotaged and shut down production and distribution, according to Symantec, a cybersecurity company that discovered the attack.

[13] Greenberg, Andy. "Hackers Gain Direct Access to U.S. Power Grid Controls, "*Wired*. (September 6, 2017) Available at https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

[14] Weise, Elizabeth. ""Intrusion - but no attack - on U.S. energy grid is a warning, says former NSA official," USA Today. (September 7, 2017). Available at: https://www.usatoday.com/story/tech/news/2017/09/06/dozens-power-companies-breached-hackers-cybersecurity-researcher-says/638503001/

> In some cases, this involved access to details about how the company operated, engineering plans and equipment, in some cases even down to the level of controlling valves, pipes or conveyer belts, said Vikram Thakur, principal research manager at Symantec, which discovered the intrusions and first published information about them in a blog posting Wednesday.

An October 10, 2017 post by security firm FireEye on its website disclosed cyberattacks on U.S. electric utilities by North Korea:[15]

> We can confirm that FireEye devices detected and stopped spear phishing emails sent on Sept. 22, 2017, to U.S. electric companies by known cyber threat actors likely affiliated with the North Korean government. This activity was early-stage reconnaissance, and not necessarily indicative of an imminent, disruptive cyber attack that might take months to prepare if it went undetected (judging from past experiences with other cyber threat groups).

A February 19, 2018 article in *RTO Insider*, "Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities, "disclosed multiple teams are actively targeting U.S. electric utilities: [16]

> The cybersecurity expert whose firm discovered the malware that caused blackouts in Ukraine in 2016 told state regulators that hackers targeting the U.S. electric industry are growing more numerous and more skilled.
>
> "There are five dedicated teams targeting infrastructure sites in North America, including eight different campaigns targeting sites," Robert M. Lee, CEO of cybersecurity firm Dragos, told the National Association of Regulatory Utility Commissioners' Winter Policy Summit on Feb. 11. "This is an extreme uptick."

Common factors in media reports of cybersecurity compromise are use of malicious code, or "malware," harvesting of credentials, and reconnaissance—instead of disruption of electric grid operations. It is rare to hear reports of insertion of malware into generation equipment, substations, or control rooms; instead malware insertions are commonly into the business systems of utilities. It is notable that none of the above described incidents would definitively be "Reportable Cyber Security Incidents" under utility interpretations of the definition in the NERC Glossary: "Cyber Security Incident that has compromised or disrupted one or more

[15] FireEye. "North Korean Actors Spear Phish U.S. Electric Companies." Website post. (October 10, 2017). Available at: https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html

[16] Heidorn, Rich. "Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities," *RTO Insider*. (February 19, 2018). Available at: https://www.rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/

reliability tasks of a functional entity." Of the media accounts above, only the *USA Today* article describes malware that might have infected operational systems and therefore would be clearly reportable under the threshold proposed in the current NOPR.

Malware Often Does Not Fall Within Reporting Thresholds

We urge the Commission to recognize that reporting of malware infection is not necessarily within thresholds set on other criteria, such as "compromise," "breach," "impact," or "disruption." The experience of another government body in setting a threshold for cybersecurity incident reporting is instructive. The European Union Agency for Network and Information Security (ENISA) implemented a "Technical Guideline on Incident Reporting"[17] in 2011 and has published annual reports since 2012. EU provisions state that Member States (MS) shall ensure that electronic communication providers will "notify the competent national regulatory authority of a *breach of security* or loss of integrity that has had a *significant impact* on the operation of networks or services." (Emphasis added.) The European incident reporting threshold is an analog to the "disruption to reliable bulk electric system operation" threshold in the current NERC reporting standard.

In its "Annual Incident Reports 2016," ENISA concluded "that malicious actions (especially cyber-attacks) are not necessarily focused on creating disruptions."[18]

> **Analysis of arising cybersecurity trends/issues**
>
> For the reporting years 2012-2016, annual reports included in total 614 incident reports with 425 incident reports (69% of total incident reports) coming from system failures. On the other side, only 34 incident reports (5,5% of total incident reports) are a result of malicious actions. Approximately 76,5% of the malicious actions consist of cybersecurity attacks, namely Denial of Service attacks, malware / viruses and network hijacks, while the rest concern deliberate damages to physical infrastructure. During all the reporting years only 3 reported incidents were caused by malware. The proportion of malicious actions (especially cybersecurity related incidents) among the total number of incidents

[17] European Union Agency For Network And Information Security. "Technical Guideline on Incident Reporting; Technical guidance on the incident reporting in Article 13a." Guideline. (Version 2.1, October 2014). Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting

[18] European Union Agency For Network And Information Security. "Annual Incident Reports 2016; Analysis of Article 13a annual incident reports in the telecom sector" Report. (June 2017). Available at: https://www.enisa.europa.eu/publications/annual-incident-reports-2016

> reported remains low due to the focus of the current regulation on the “availability” of services and networks, meaning *mostly disruptions*.
>
> *Considering the above we may conclude that malicious actions (especially cyber-attacks) are not necessarily focused on creating disruptions in Telecom*, a conclusion that has already been presented in previous versions of this report. But, what we also can conclude is that, under the current form of Art. 13a within the Electronic Telecommunication Framework Directive, we do not have a very good overview of the cyber-attacks affecting the telecommunication infrastructure in EU. Although the present incident reporting scheme currently does not allow us to see the whole picture, external sources (public reports, statistics, online articles etc.) on Telecom incidents confirm an increasing trend as regards cyber-attacks. According to PwC’s Global State of Information Security, 2016 18, IT security incidents in the telecom sector increased 45% in 2015 compared to the year before.
>
> However, for the first time in the six year analysis of annual incident reports we see *malware as the detailed cause*, with the most impact in terms of average duration and user hours lost. (Emphasis added)

We learn from European experience that very few malware incidents are reported, but when malware is the cause of a disruption, it has the most impact.

We importantly observe that malware infection will likewise not necessarily fall within the proposed threshold set forth in the NOPR: “mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s ESP or associated EACMS.”[19] We urge FERC to set a reporting threshold that includes required reporting of all malware infections, both inside and outside Electronic Security Perimeters. The best threshold for reporting of malware is simple: detection of malware wherever it is found. This is especially important because much malware is of the “Trojan Horse” or Advanced Persistent Threat (APT) varieties that are purposely inserted to lie dormant until triggered at a later date when effects will be most catastrophic—for example, during a major hurricane, or a severe solar geomagnetic storm, or prior to a combined-arms military action.

[19] NOPR at 19.

Responses to FERC Comment Prompts

Other responses for comments sought by FERC are below, organized by prompt in bold.

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

As we explain elsewhere in this comment, the modifications proposed to improve the reporting of cybersecurity Incidents are unlikely to have any significant positive effect. The number of reported incidents is likely to remain minimal. Unless the NOPR is substantially revamped, much of the time and effort expended on standard-setting and rulemaking could be unproductive.

The Commission proposes to direct that NERC modify the CIP Reliability Standards to specify the required content in a Cyber Security Incident report. We propose that the minimum set of attributes to be reported should include: (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident…The Commission seeks comment on this proposal and, more generally, the appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities.

In developing the required content in a cybersecurity incident report, we respectfully suggest that the Commission leverage work already done by the federal government. US-CERT has published “Federal Incident Notification Guidelines” with the following information elements required when notifying US-CERT of an incident:[20]

1. Identify the current level of impact on agency functions or services (Functional Impact).
2. Identify the type of information lost, compromised, or corrupted (Information Impact.)
3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
4. Identify when the activity was first detected.
5. Identify the number of systems, records, and users impacted.
6. Identify the network location of the observed activity.
7. Identify the point of contact for additional follow-up.
8. Submit the notification to US-CERT.

The following information should also be included if known at the time of submission:

9. Identify the attack vector that led to the incident.
10. Provide any indicators of compromise, including signatures or detection measures developed in relation to the incident.
11. Provide any mitigation activities undertaken in response to the incident.

At present time, only two of the Commission’s proposed minimum set of reportable attributes overlap with the US-CERT elements:

(1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve;

(2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident.

We propose that Commission attribute No. 3, “the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident,” be added to the US-CERT list.

[20] United States Computer Emergency Readiness Team (US-CERT). “US-CERT Federal Incident Notification Guidelines.” Guidelines. (Effective April 1, 2017). Available at: https://www.us-cert.gov/incident-notification-guidelines

The Commission should recognize that when malware is the attack vector, utilities have a perverse incentive to delay mitigation of the malware, because mitigation may necessitate shutdown of operational systems, causing increased costs or lost revenues, especially for merchant generators and transmission companies. A January 8, 2018 article in *EnergyWire*, "Gadfly advocates win a round on cyberattack rules," confirms this issue:[21]

> Asked whether utilities would be likely to remove malware on their own, without a specific requirement to do so, Miller said, "I've been to too many generation plants that still have Conficker running around in them," referring to a 9-year-old virus that attacks Microsoft operating systems. "If it's not impacting operations, they don't care, because the effort to take the systems offline to remove [the malware] is an outage, downtime, impact.

Accordingly, Resilient Societies proposes that an improved cybersecurity reporting standard require a second reporting attribute over and above the US-CERT attributes: "a schedule and expected completion date for additional mitigation activities."

In addition, the Commission seeks comment on whether to exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold.

Excluding Electronic Access Control or Monitoring Systems (EACMS) from the Commission directive could exempt reporting of attempted compromises. Clearly, breach of a firewall (one of the most common types of EACMS) is a serious cybersecurity incident that should be reportable.

The Commission also seeks comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards. Specifically, we seek comment on whether a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure would effectively address the reporting gap and current lack of awareness of cyber-related incidents, discussed above, among NERC, responsible entities and the Commission, and satisfy the goals of the proposed directive.

[21] Behr, Peter and Sobczak, Blake. "Gadfly advocates win a round on cyberattack rules," *EnergyWire*. (January 8, 2018). Available at: https://www.eenews.net/stories/1060070313

Examination of NERC Rules of Procedure Section 1600 shows the intent of rule is to facilitate one-time requests for data. Section 1602.1, Procedure for Authorizing a NERC Request for Data or Information, reads:

> A proposed request for data or information shall contain, at a minimum, the following information: (i) a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements; (ii) a description of how the data or information will be collected and validated; (iii) a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("reporting entities"); (iv) the schedule or due date for the data or information; (v) a description of any restrictions on disseminating the data or information (e.g., "confidential," "critical energy infrastructure information," "aggregating" or "identity masking"); and (vi) an estimate of the relative burden imposed on the reporting entities to accommodate the data or information request.

Notably, Subsection (iv) specifies "the schedule or due date for the data or information"— "schedule" and "due date" are clearly singular nouns. This existing NERC procedure would be a poor fit for a standing order for data on cybersecurity incidents that occur continually.

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

In an ideal world, reporting of cybersecurity incidents would take place at machine-speed, within seconds, or even microseconds, of the incident taking place. We suggest that the Commission word its final order, including the list of reportable attributes, to allow and preferably to require automated reporting, at least for an initial report.[22] Subsequent and more complete reports, in the timeframe of several days, may require human intervention. Also, the definition of "incident" should be expanded to explicitly include detected Trojan Horse infections and Advanced Persistent Threat (APT) malware.

[22] The Department of Commerce National Institute of Standards and Technology (NIST) has developed standards for automated cyber incident reporting, including automated "vulnerability scanning." See for example, David A. Waltermire, *et al.*, *The Technical Specification for Security Content Automation Protocol (SCAP): SCAP Version 1.3,* NIST Report SP-800-126, February 14, 2018, including Section 5.2 on "vulnerability scanning" at pp. 43-44.

We especially commend for Commission's consideration the assessments and recommendations for "pilot programs" to include automated near-real-time reporting of cyber incidents impacting both the electric utility and the financial industry. Such a program for the U.S. electric utility industry is favorably considered in the August 2017 Report to the President by the National Infrastructure Advisory Council, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.[23] The NIAC Report (at page 3) endorses a pilot program for "machine-to-machine information share technologies, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed."[24]

The potential for automated cyber incident reporting opens parallel potential for automated or automated-plus-human assessment reporting at network or near-network speeds.

When new cyberattack campaigns can develop in hours or days or weeks, an annual summary report to the Commission would not be in the public interest. We suggest quarterly, or even monthly, reports from NERC to the Commission.

Moreover, FERC may seek additional voluntary reports from other recipients of cyber incident information sharing, including the industry-sponsored E-ISAC managed by NERC; and components of the U.S. Department of Homeland Security: US-CERT, ICS-CERT, and the National Cybersecurity and Communications Integration Center (NCCIC).

We encourage the FERC Commissioners to issue a Policy Paper emphasizing the primary goal of cyber incident reporting and mitigation is to attain early warning, situational awareness, and protection of the reliable operation and prompt recovery of the bulk power system from cyber incidents, whether or not malicious in origin or intent.

[23] National Infrastructure Advisory Council. "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report." Report. (September 1, 2017). Available at: https://www.dhs.gov/sites/default/files/publications/transmittal-letter-potus-niac-securing-cyber-assets-508.pdf

[24] The August 2017 NIAC Report further proposes: "Threat information and mitigation must move at network speed. Advances in machine-to-machine information sharing and automated mitigations show great promise." *Ibid.*, at p. 8.

Registered entities that report cyber incidents promptly and in good faith should be shielded from liability and fines. The Critical Infrastructure Protection (CIP) standards now in effect are insufficiently protective and may be unintended barriers to the network-based information sharing needs of the future.

Request for Technical Conference Held in Public Session

Too often in the past, rulemakings for reliability standards appear to have facilitated closed negotiations between FERC and NERC, with other public stakeholders denied both information and effective participation. In regard to the current rulemaking, cybersecurity vendors such as Symantec, Dragos, FireEye, and Cylance have knowledge of campaigns against U.S. electric utilities as well as critical infrastructures abroad. We respectfully request that the Commission hold a technical conference in public session, with cybersecurity firms as panelists, to obtain a more accurate picture of cybersecurity risk—especially risk from malware—and opportunities for network speed automated protections, before making a final ruling.

It is our belief that the vast majority of malware signatures currently in possession of ICS-CERT and US-CERT were reported not by electric utilities directly, but through the systems of cybersecurity vendors. Questioning of staff at ICS-CERT and US-CERT in public session could confirm that voluntary reporting of malware signatures by electric utilities directly would provide opportunities for significantly improved "best practices," even before an enhanced reliability standard is implemented.

Finally, testimony in a public technical conference could bring forth a better threshold for cybersecurity incident reporting—a threshold that does not solely depend on compromise of Electronic Security Perimeters or Electronic Access Control or Monitoring Systems.

Supporting Recommendations of Applied Control Solutions

Resilient Societies also endorses the recommendations submitted in this Docket by a national expert on control systems, Joseph Weiss of Applied Control Solutions, LLC:

1. Require utility personnel to identify all electronic communication impacts that could affect grid reliability as being cyber-related, whether malicious or unintentional.
2. Require utilities not NERC, to disclose to FERC, ICS-CERT, the National Cybersecurity and Communications Integration Center (NCCIC), and the utility industry all control system cyber incidents in plant, transmission, distribution, or SCADA operations in an expeditious manner. This is because many cyber-related events are not unique to just one utility or facility.
3. Require training by plant and substation staff to better understand control system cyber security and to recognize upset conditions that could be cyber-related.
4. Require utility IT and physical Security Operations Centers (SOCs) to coordinate with plant and substation Operations Centers to better coordinate what upset conditions may be cyber-related."

Reliability Standard to Be Set By a Necessary Deadline

NERC has a procedure to allow an urgently needed reliability standard to be set by a necessary regulatory deadline:[25]

> **Section 16.0: Waiver**
>
> While it is NERC's intent to use its ANSI-accredited Reliability Standards development process for developing its Reliability Standards, NERC may need to develop a new or modified Reliability Standard, definition, Variance, or implementation plan under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn't sufficient time to follow all the steps in the normal Reliability Standards development process.
>
> The Standards Committee may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
>
> - In response to a national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber attack on the Bulk Electric System;
>
> - Where necessary to meet regulatory deadlines;

[25] NERC. "Standard Processes Manual, VERSION 3." Effective: June 26, 2013. Available at: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Given several years of data that remains unreported under the current cybersecurity incident reporting standard, and given the national security situation where the U.S. electric grid lacks effective cyber defenses (according to the Defense Science Board's Cybersecurity Task Force), we respectfully request that FERC set a regulatory deadline for an improved Cyber Security Incident Reporting Reliability Standard.

Conclusion

The current NERC cybersecurity reporting standard fails to protect the public from catastrophic grid outages, with zero reportable cybersecurity incidents in multiple years. Even NERC admits that the "mandatory reporting process does not create an accurate picture of cyber security risk…"[26] Official government reports and disclosures by cybersecurity vendors show that multiple cyberattack campaigns are threatening the U.S. electric grid; these campaigns often include malware infections.

Malware commonly infects business systems, but infections are much less common in the operational systems of utilities—those systems behind Electronic Security Perimeters and Electronic Access Control or Monitoring Systems. Compromise of an operational perimeter is a deficient threshold for cybersecurity incident reporting, especially reporting of potential or actual malware infection. Most attackers are smart enough to not breach perimeters until the time of a full-scale attack. The best threshold for reporting of malware is simple: detection of malware wherever it is found. Moreover, cyber incidents, including impacts or attempted impacts upon control systems, whether malicious or not, should be within a class of required cyber incident reporting, preferably at network speeds.

Opportunities for automated reporting and automated protection initiatives are in the public interest. The Commission has the authority to augment the identification and reporting of cyber incidents under Section 215 of the Energy Policy Act of 2005. The Commission needs to embrace protective technologies and apply them without discrimination to all registered entities.

[26] NERC, "2017 State of Reliability Report." (June 2017), p. 4. Available at: .http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MAS TER_20170613.pdf.

The Commission should take notice of multi-year NIST and US-CERT initiatives to develop attributes for reporting characteristics of cybersecurity incidents. The US-CERT attributes are a good starting point for an improved cyber incident reporting reliability standard. Moreover, the Commission has an opportunity now to encourage and accelerate machine-to-machine pilot reporting programs for automated protections of a 21st century electric grid.

We respectfully request that FERC establish new transparency in rulemaking and standard-setting by holding a public technical conference to take testimony from cybersecurity vendors; their experts have broad and direct knowledge of cybersecurity risks, beyond knowledge of any single utility or trade association. We also urge the Commission to invite the National Infrastructure Advisory Council Task Force on Cyber Asset Protection to share their insights on opportunities for automated monitoring, scanning, and reporting, and automated defenses for cyber assets. Based on expert testimony and public comments in this rulemaking, the modifications proposed in the NOPR could be substantially revamped.

With this standard setting, FERC has the opportunity to improve the reliability standard-setting and approval process, acting not in the narrow economic interest of regulated utilities, but in the public interest.

Respectfully submitted by:

Thomas S. Popik

Thomas S. Popik, Chairman
thomasp@resilientsocieties.org

Wm. R. Harris

William R. Harris, Secretary,

williamh@resilientsocieties.org

Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org

Appendix 1: Letter to NERC Board of Trustees

Foundation for Resilient Societies
52 Technology Way
Nashua NH 03060
www.resilientsocieties.org

May 12, 2016

Frederick W. Gorbet, Chair
Roy Thilly, Vice Chair
Gerald W. Cauley, President and CEO
Paul F. Barber
Janice B. Case
Robert G. Clarke
Board of Trustees
North American Electric Reliability Corporation
3353 Peachtree Road, N.E. Suite 600, North Tower
Atlanta, GA 30326

Kenneth W. DeFontes, Jr.
David Goulding
George Hawkins
Kenneth G. Peterson
Jan Schori

Dear Trustees:

We are writing in regard to your Board's pending review of the North American Electric Reliability Corporation (NERC) *State of Reliability 2016* report, scheduled for approval at the May 13, 2016 Board meeting. We are concerned this report may present misleading statistics on reportable cybersecurity incidents for the Bulk Power System during calendar year 2015.

Government policymakers and the public increasingly recognize the threat of cyberattack on critical infrastructure such as the electric grid. In December 2015, a sophisticated cyberattack took down portions of the Ukrainian electric grid. An April 2016 poll by the Pew Research Center indicates 72% of Americans view cyberattacks from other countries as a "major threat." An October 16, 2015 article published by CNN, titled "ISIS is attacking the U.S. energy grid (and failing)," disclosed that the Islamic State seeks to hack American electrical power systems.

NERC staff told us the draft *State of Reliability 2016* report has been supplied to your Board of Trustees. Section 4 of the NERC By-Laws clearly states that material provided to the Board must be publicly posted within 24 hours: "all nonconfidential material provided to the board, shall be posted on the Corporation's Web site, and notice of meetings of the board shall be sent electronically to members of the Corporation, within 24 hours of the time that notice or such material is given to the trustees." Moreover, Section 215 of the Federal Power Act mandates that NERC, as the Electric Reliability Organization (ERO), must "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties."

NERC's legal staff has refused to make available the *State of Reliability 2016* report, maintaining it is "confidential." NERC's ongoing practice of restricting access to Board-provided materials—even for several days after the material is approved by the Board for public distribution and therefore cannot be "confidential"—appears to be a clear violation of NERC's own By-Laws, as well as federal law.

Conversely, were NERC to make the *State of Reliability 2016* report publicly available via the NERC website within 24 hours of submittal to the Board, stakeholders would have an opportunity to identify biases or omissions, helping the Board to improve the accuracy and utility of reliability metrics. We ask you to release the *State of Reliability 2016* report immediately. If the NERC *State of Reliability 2016* report follows the pattern of last year's report, it may contain materially misleading statements in regard to the number of reportable cybersecurity incidents. In the *State of Reliability 2015* report, NERC represented that only three (3) reportable cybersecurity incidents had occurred for the Bulk Power System in all of 2014. Our understanding is that the number of reportable cybersecurity incidents for 2015 may likewise be a very low number.

In contrast, in Fiscal Year 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security received 79 reported cybersecurity incidents from the Energy Sector. In Fiscal Year 2015, ICS-CERT received 46 reported cybersecurity incidents from the Energy Sector. It is improbable that electric utilities are immune from cybersecurity incidents that affect the Energy Sector generally. We also note that Admiral Michael Rogers, Director, National Security Agency and Commander of U.S. Cyber Command, testified to Congress on November 20, 2014 that multiple foreign nations can take down the U.S. grid—this statement is inconsistent with trivial numbers of cybersecurity incidents reported to NERC by electric utilities.

At the January 28, 2016 FERC Technical Conference on Supply Chain Risk Management, a cybersecurity expert testified that "BlackEnergy" malware is pervasive within the North American electric grid. This is the same family of malware used to acquire credentials to black out the western Ukrainian electric grid.

According to NERC Critical Infrastructure Protection standards and Glossary of Terms, a Reportable Cyber Security Incident is "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." When malware is detected in operational system of an electric utility, clearly a "compromise" has occurred. Malware infection may require a switch to manual operations to ensure security. Additionally, shutdown or isolation of systems may be required to remove malware. Therefore, detected malware infection should be a clear case of a "Reportable Cyber Security Incident." If NERC has a pattern and practice of permitting regulated entities to opt out of reporting malware infections and other cybersecurity incidents, this could lead to misleading statistics in the *State of Reliability* reports.

When misleading statistics are given to government policymakers, this can forestall remedial legislation and federal rulemaking necessary to protect critical infrastructures and public safety. Before approving the *State of Reliability 2016* report, we respectfully request that the NERC Board of Trustees determine if incomplete cybersecurity incident reporting by electric utilities has obscured the true risk of cyberattack on the North American electric grid.

Sincerely,

Thomas S. Popik

Thomas S. Popik
Chairman, Foundation for Resilient Societies

Document Content(s)

193 Southdown Road
Edgewater, MD 21037

February 6, 2018

Federal Energy Regulatory Commission
888 First Street NE
Washington DC 20426

Sirs,

Enclosed, please find Isologic LLC filing on the NOPR "Cyber Security Incident Reporting, Reliability Standards" Docket Nos. RM18-2-000 and AD17-9-000, Issued December 21, 2017.

Submitted,

George R. Cotter

George R. Cotter
Isologic LLC

cc:

Margaret Scott
Office of Electric Reliability
Federal Energy Regulatory Commission

Kevin Ryan
Office of the General Counsel
Federal Energy Regulatory Commission

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOPR Cyber Security Incident Reporting
Reliability Standards — Docket Nos. RM18-2-000 and AD17-9-000
Issued December 21, 2017

Isologic LLC respectfully submits these comments and recommendations on the subject NOPR which is largely in response to the Foundation for Resilient Societies' filing of January 13, 2017 titled "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. ***Isologic LLC respectfully urges the Commission to revise its proposed rule, particularly for so-called Low Impact Cyber Assets, in light of the information and recommendations in this filing.***

Introduction

Since the passage of the Energy Policy Act of 2005, amending the Federal Power Act, the undersigned, often in collaboration with the Foundation for Resilient Societies, has frequently petitioned the Commission on the creation of Critical Infrastructure Standards, their contents, vulnerabilities and threats, and most importantly, their role in safeguarding power systems for the nation. Such filings have been comprehensive, well-documented and unquestionably in the interests of the Nation.

This filing responds to the specific changes proposed in the NOPR of 21 December 2017. However, the author of this filing now concludes that the Critical Infrastructure Protection (CIP) process, and results, over the last decade, have finally hit their nadir. CIP Standards have simply failed to protect the Bulk Electric System and therefore the Distribution System, and therefore the infrastructures, institutions and citizens nearly totally dependent on the National Grid. Since 2012, Russia has conducted operations against the Grid, performing reconnaissance, collecting intelligence, and developing sophisticated attack systems, details summarized in this filing. The industry and NERC response, in agreement with DOE/OE (in apparent violation of its own standards[i]), has been to suppress almost all incident reporting with "tongue-in-cheek" statements that there has been no damage inflicted on the BES (Russian choice, not CIP Standards). With rare rebuttals, FERC has followed along, this NOPR being a current example.

(Q) How is this possible, how can the nation now find it electric power system near totally defenseless and the primary target of one of its principal adversaries? ***(A)*** Key failures in CIP Standards development, unwillingness of the industry and NERC to take collective actions for defense, vacuous assertions on information sharing and non-existent "resiliency" as a counter, and failure of FERC, other overseers, the Congress, and two administrations to understand the inevitable consequences of over a decade of CIP inadequacy since the EPA of 2005. In addition to addressing the December 21, 2017 NOPR, this filing will set the record straight on major CIP failures in the hope that the current Commission will reduce the risk of a power crisis (should Russia choose to attack).

Let's start with the EPA of 2005, section 215. It states:

"(8) The term 'cybersecurity incident' means 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." (Emphasis added).

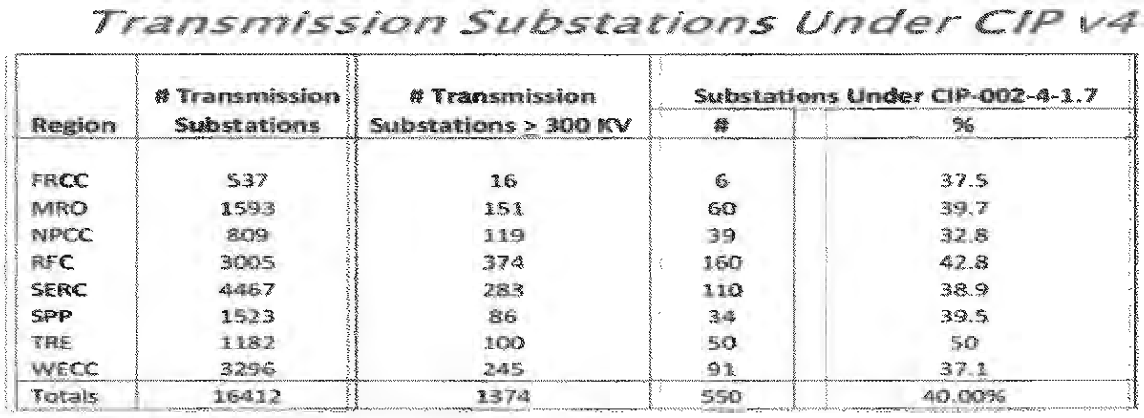
Despite the specific inclusion of ***"communications networks"*** in the law, FERC accepted a NERC recommendation to exclude these critical connections from CIP categorization, i.e., ***"Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.",*** one of only four major exclusions of CIP-002-5.

The law provides no such exception; one intended by NERC to shield BES utilities from unwanted cybersecurity regulation. The massive communications networks within and among utilities, including unsecured Internet connectivity, represent a major vulnerability, unprotected by CIP standards. ***This was, and is, a deliberate effort to circumvent the law.*** Addressing all communications networks in CIP would have been the glue that defined the BES strategy as an integrated secure system for over 1400 independent "responsible entities", forced interconnected utilities to address mutual threats, permitted a Grid-wide Situational Awareness structure, provided a foundation for ultimate critical national defense by DoD, established a solid basis for addressing, with vendors, product vulnerabilities, permitted a rational policy on Internet connections, a national capability in secure systems, and a myriad of additional advantages to security modernization. ***Instead, this singular violation of the EPA, by the industry, NERC and FERC, has made a substantial, if unintentional, contribution to the nation's adversaries.***

2. CIP Categorization

Let's examine what else is included or excluded from CIP Standards, and therefore incident reporting. CIP-002-5 categorizes all BES Cyber Assets as Low, Medium or High relative to impact on the BES, with very specific definitions and metrics for High and Medium categories. To be categorized as a BES Low Impact Cyber Asset (its exact composition is left to the utility owner to describe), the minimum requirement is to satisfy a 300kva requirement in terms of the minimum aggregate power at the facility. Also, the potential loss of the asset must have an impact on BES reliability within 15 minutes of an incident. If not, it is not a Cyber Asset and therefore not subject to incident reporting. Multiple cybersecurity vulnerabilities, incidents, malware threats, dangerous real-world examples, reveal Russian focus on industrial control systems (ICS) at so-called BES Low Impact facilities, collectively the soft underbelly of Medium and High Impact Cyber Assets. It is therefore critical (despite NERC disclaimers) to assess these collective vulnerabilities, to validate what passes as CIP Standards. How many satisfy the power and 15-minute test, and at which utilities? How else would compliance authorities evaluate compliance without knowing these basic facts. The view that loss of such Cyber Assets, individually, would have only low overall impact on the BES absolutely begs the question of the effect on the BES of simultaneous loss of dozens, hundreds, thousands of such cyber assets.

During consideration of proposed CIP V4 Standards, this issue seriously concerned FERC. NERC was tasked to collect the data on inclusions and exclusions for FERC assessment of CIP V4. Fortunately, NERC put that data in the public domain[ii], which permitted construction of the following chart summarizing the status for CIP v4 Transmission Systems in each reliability region:



Transmission Substations Under CIP v4

Region	# Transmission Substations	# Transmission Substations ≥ 300 KV	Substations Under CIP-002-4-1.7	
			#	%
FRCC	537	16	6	37.5
MRO	1593	151	60	39.7
NPCC	809	119	39	32.8
RFC	3005	374	160	42.8
SERC	4467	283	110	38.9
SPP	1523	86	34	39.5
TRE	1182	100	50	50
WECC	3296	245	91	37.1
Totals	16412	1374	550	40.00%

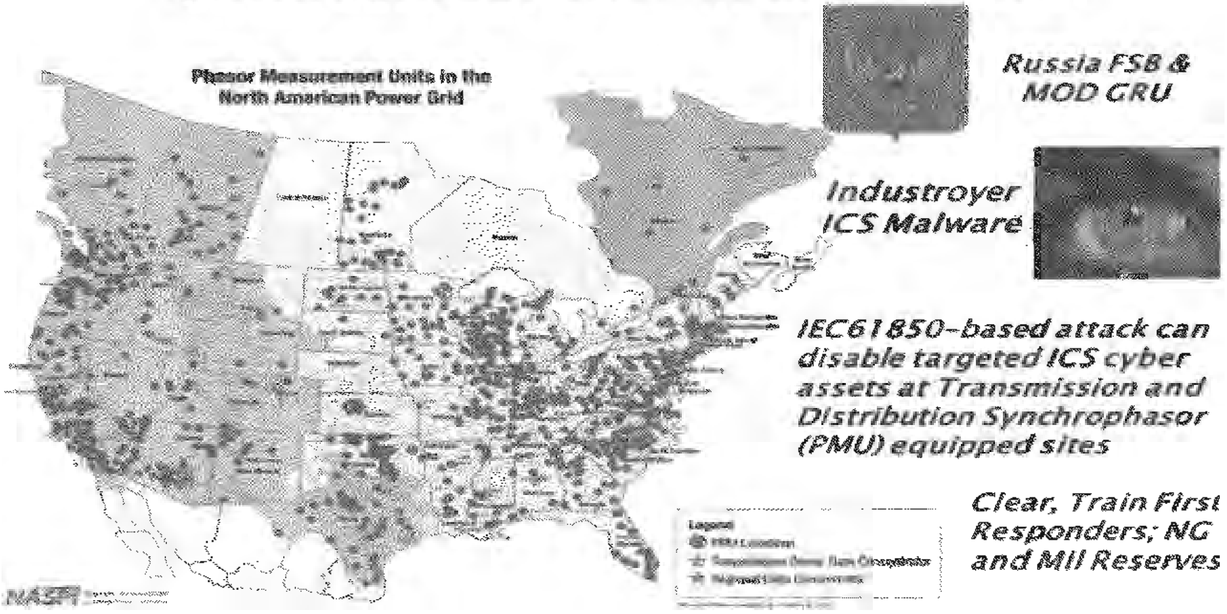
We can see that only 1374 of a total of 16,412 BES Transmission Substations qualified for CIP Standards based on Kv power minimums (over 90% excluded) and of the qualifiers, only 550 (40%) were estimated by their utilities to be critical to BES Reliability. These judgments were validated by their Reliability Region, i.e., the Compliance Authority and by NERC.

When CIP v4 gave way to CIP v5/6, these basic voltage/15 minute requirements did not change with the transition. NERC will protest that this display does not reflect CIP v5 coverage, but rest assured, they will not voluntarily provide the current coverage statistics. ***FERC should, of course, insist on a full exposure of Low Impact Cyber Asset coverage under CIP, since it has the authority, and obligation, under Section 215 of the EPA.*** ESPs, let alone EACMSs do not exist at the majority of Transmission substations. Further, attacks on Low Impact Transmission systems will be the number one Russian target since it would have maximum impact on the nation's urban populations and national security organizations. The overall pattern of Russian incursions shows this to be true.

(Q) Can survivability of less than the 10% of Transmission Substations theoretically engaged in CIP-directed incident reporting, ensure survival of the BES and its dependent Distribution systems? *(A)* It is truly a pointless question when vulnerabilities, confused connectedness, threats and Internet dependencies are mutually involved. In this context, examine the following map of Synchrophasor facilities in North America, now the major data source for real-time management of interconnected transmission and distribution power flows among utilities. Many of these sites are directly connected to the Internet. How well do users, other critical infrastructures, and National Defense organizations, understand the inadequacy of CIP Standards, and should they trust the proposed "incident reporting" standards? But of course, they are kept in the dark on all this, few would be aware of the "NOPRs" that are the subject of this paper.

Yes, it would take a large cyber army to disable a nation-wide complex such as the PMU sites display on the map included below. But major national tragedies can be created with far less an effort. How does FEMA deal with 8 million people trapped in a blacked-out Manhattan?[iii] How does a national government function with no power available in Washington D.C.? How seriously is the Nation affected with a disabled or captured financial system? Think of major medical facilities running on only emergency power systems. How many people would die if the FAA air traffic control system was suddenly shut down, or taken over? Yes, Russia could be successful on any of the foregoing.

Synchrophasor Sites In Electric Grid



Russia FSB & MOD GRU

Industroyer ICS Malware

IEC61850-based attack can disable targeted ICS cyber assets at Transmission and Distribution Synchrophasor (PMU) equipped sites

Clear, Train First Responders; NG and Mil Reserves

Even a cursory examination of Russian malware development and testing against US Grid systems since at least 2012 would satisfy any skeptic on the threat to this nation's critical communities. ***Industroyer,*** cited on this map, is but one of sophisticated Russian malware packages. It employs a major international interoperability standard ***(IEC 61850)*** that can be tailored to achieve the type of selective control for the "incident" examples cited above. Note, the Russians have used ***Industroyer*** in their favorite cyber testing grounds, the Ukraine Grid. Citizens would ask the question, "How could such conditions occur?" They will find the answers in this filing.

II. Malware Issues

The Foundation's filing of January 13, 2017[iv] provided an extremely detailed discussion of issues faced by utilities in malware detection, mitigation, removal and incident reporting. Only incident reporting is addressed in this NOPR (rather incompletely) and FERC asserts that all other issues are dealt with adequately in other CIP standards. This assertion is not backed up with examples of how utilities can effectively manage the malware threat. Frankly generalities are a poor substitute for facts, technical examples, how utilities will deal with actual threat vectors. This filing will not repeat the Foundations' comprehensive arguments; but will supplement that treatment with additional background and specific recommendations for follow-up by FERC.

1. Detection

To appreciate the sophistication of adversaries' cyber attacks, one need only examine the development of FURTIM[v], Russian malware that examines over 400 protective systems, determines if a safe bypass of those systems exists before proceeding, and if not, it backs out of, or resorts to different penetration techniques. Not much is known about ***Furtim,*** its further development and testing has not been detected. (Which makes ***Furtim*** itself a major detection challenge.) The extreme generality of CIP Standards often leaves utilities uncertain of vulnerabilities and therefore indifferent to threats. However, there is no effective argument against standards which require utilities to employ active measures for detection of "known malware". Major threats are addressed by security firms, ICS CERT provides Yara software to identify these[vi]. ESP and EACMS requirements must specify such safeguards, whitelisting and blacklisting are tools that exist for this purpose. ***This NOPR should task NERC to develop standards governing this critical protective step, i.e., Detection***

In examining revisions to CIP 005, 010 and 013 as a consequence of Order No. 829, the damper on that order's intent[vii] is***: "However, to be clear, we reiterate the statement in the NOPR that any action taken by NERC in response to the Commission's directive to address the supply chain-related reliability gap should respect section 215 jurisdiction by only addressing the obligations of responsible entities"*** and ***"not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities."*** Mindful of the non-concurrence of Commissioner LaFleur to the summary issuance of Order No 829, the policy should be precisely the opposite. Utilities should use every tactic available to convince vendors that malware in products supplied to the utility will not be tolerated. Many such tactics are available, indeed too many to enumerate here, including blacklisting.

The enormous dependency of OT vendors on commercial IT systems obscures the major vulnerabilities from such sources, utilities need to guard against this. ***However, the most basic, systemic flaws never receive attention by OT vendors, the industry, individual utilities, its protectors, directives from FERC, and critically, in the charade of CIP Standards.*** Take for example, insecurity of IT Operating Systems[viii] (Microsoft Windows, MacOS, Linux) which, if ignored in fundamental system hygienics by users of commercial OT systems, makes a mockery of most other security steps for protection of Cyber assets.

However, CIP requirements focus entirely on very general procedural factors, Access Controls, Change Management and Risk Management. There is nothing specific concerning known threats, technical characteristics, sources of specific threat information aligned to specific supply chain vulnerabilities and communication network connectivity to vendors. A concerned utility wishing to prevent supply chain attacks will not find the pointers to solutions anywhere in these gross policy statements. ***The requirements for these CIP Standards should be revised to provide far more specific guidance such as promulgated by NIST[ix], based on evidence accumulated in open sources on Supply Chain vulnerabilities, threats, best practices. Detection of malware is a major responsibility of all "Responsible Entities".***

2. *Malware Mitigation*

a. *The Utility's Role*

Mitigation of malware can take many forms, prevention of known malware threats, defenses against its insertion in IT and OT systems, detection (as described above) and removal. Every utility should have a comprehensive malware mitigation program. Like a germ-free hospital, utilities should have comprehensive anti-viral systems and procedures and should systematically examine operations with 100% prevention as a goal. Periodic penetration testing is essential, with professional Red Teams. Known threats, particularly if they appear focused on a utility's vulnerabilities, should be studied and where feasible, threat-focused protective systems applied. Logs should be examined periodically by experienced forensic experts to detect unusual activity that may be indicative of malware implants, or future targeting. All operations personnel should be trained in malware detection, such training should not be onerous. Malware removal should be left to experts who might reverse engineer its insertion to better prevent recurrences. National Guard cyber warriors should be trained as First Responders. Security systems should be thoroughly understood by utility cyber/IT personnel with emphasis on current and past vulnerabilities in such systems. Patches to security systems should be assiduously applied.

Mitigation efforts that surface malware should be carefully documented. Utility experts should be particularly sensitive to malware that reports detections to attackers; forensic experts might be important to the malware removal process[x]. Procurement, maintenance, upgrades and replacements of IT and OT systems represent opportunities for malware insertion and should be subject to critical examination by cyber defense personnel.

In training personnel in malware mitigation, there should be emphasis on real world examples taken from actual US incidents. This education should emphasize the danger to operations and the critical role that can be played by all personnel in prevention. Use of experts in malware forensics should be strongly encouraged. Training should include hands-on examples in malware detection, mitigation, removal and incident reporting. It is important to emphasize the competencies of the utility's adversaries, forbidding operational personnel from attempting counter strategies, so-called active defenses. That's a game for trained cyber warriors. Shun vendors who propose attacking attackers.

If malware cannot be removed, it must still be fully "incident reported" with reasons for non-removal provided. Obviously, this is more important than removable malware, since other utilities may be similarly infected, additional protections may be inferred, need to alert national authorities.

b. NERC and FERC's Role

Reasonable questions are "***do these oversight organizations, NERC and FERC, really understand Grid vulnerabilities, do they appreciate the threats and how intensely the nation's adversaries study and target them? Do they realize the magnitude of risk to institutions when power is denied them? Do they prioritize cybersecurity on a par with other reliability, tariff, modernization activities?***" Of course such answers would be positive. So let's test their understanding, as follows: Click on the following URL. If you're reading a paper copy, insert the URL in your browser. https://www.smartgrid.gov/recovery_act/program_impacts/applications_synchrophasor_technology.html

What you will observe is a map of the US with Reliability Regions and some sub-Regions outlined. You will note a few widely dispersed utility facilities and real-time, every four seconds, metrics on frequency stability averages for the region. Yes, this is a valuable tool for nation-wide operational management of one of the most critical metrics in power transmission/distribution among utilities, maintaining stability of 60 cycle AC. How does this work? Where does the data come from? How secure is this operation, connectivity, the exchange, the data flows, the computation, the nation-wide accesses? All are logical cybersecurity questions that responsible organizations should be capable of asking.

Regrettably, beyond its obvious value, it's all bad news. The data is from over several hundred widely dispersed unprotected phasor measurement systems, bi-directionally networked across the Internet, data flows are 'en clair', not secured, and the entire operation is accessible to anyone including the nation's adversaries. A reasonable assumption is that Russia is well-aware of this infrastructure, and has the tools and trained cadre to assume control of it. This is a serious security hole in the nation's grid, so another reasonable assumption is that NERC and FERC are not aware of this major vulnerability, or have ignored it.

What should the nation's citizens conclude about this flagrant security situation, and relatedly, this Notice of Proposed Rule on Incident Reporting? How should it be rewritten to begin to address the nation's critical dependency on commercial power? What do they say to the nation's leadership, the Administration, the Congress? Citizens will find some of the answers to these questions, below. FERC should insist that CIP Standards task each "Responsible Entity" to produce and use a comprehensive mitigation plan for its cyber assets.

3. ***Malware Removal***

In its opposition to Foundation's filing of January 13, 2017, the utility ITC claimed[xi], among many reasons, that it was too expensive for a utility to be required to remove known malware from its systems. This should have been contested by FERC in its pre-NOPR assessment since It should be standard practice for utilities, upon recognizing or being informed of malware penetrations, to take immediate steps to remove it from their systems. Upon learning of malware targeting Grid systems, mandatory testing for its presence should be required of all utilities and if feasible, it should be completely removed by cyber professionals. Major malware identification almost always comes with directions on removal, from security firms, from US CERT[xii]. Compliance monitors should penalize any utility that tolerates known malware, regardless of its impact on BES reliability since Implanted malware may also be a threat to connected utilities, or worse, power clients.

These principles should be promulgated by FERC and incorporated in CIP Standards.

4. ***Incident Reporting***
   a. ***limitations***

FERC asserts that additional incident reporting requirements should be limited to those involving ESPs, or EACMS (note, the latter's conditional inclusion is not defined[xiii].) This is a traditional NERC cop-out; 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. ***Further, for credibility reasons, NERC must, convincingly, refute the evidence in this filing that about 90% of BES Transmission facilities are excluded from CIP Standards, and therefore, incident reporting.***

FERC defends limiting incident reporting to those involving ESPs, asserting that incidents involving all other cyber assets (presumably Middle and High impact) are covered by other standards or "work underway". Russian reconnaissance has turned up dozens of ways to negate "ESPs", through other connectivity, phishing for credentials, control system vulnerabilities, supply chain accesses already in-hand, penetration of data links (contents not examined at ESPs or EACMSs), zero-day flaws in IT systems that support ESP protections, cryptographic flaws, back doors in vendor-supplied security systems, and more. Read ICS CERT's advisories and alerts for details. With no standards for Low Impact

ESPs, we are asked to believe that over 3200 utilities can independently prevent damage or control system takeover affecting the entire BES (and therefore power distribution to the nation's users.) Note that the nation has no higher-level defenses in place for Grid protection, no established Deterrence Policy aimed at Russia, China or other competent adversaries despite proven targeting of the US. Federally, DHS and DOE leave federal incident investigations to the FBI, relying on vendors and "information sharing" for national protection.

NERC further asserts that proposed Reliability Standard CIP 003-7 (along with existing or proposed changes to other Standards) will satisfy additional requirements for incident reporting involving Low Impact Cyber Assets, approval pending responses to the NOPR, Docket No. RM17-11-000 Issued October 19, 2017. A careful reading of NERC's proposal reveals many uncertainties on utilities implementation, attributed by NERC to the wide variety of systems, technologies, communications, et al. employed at this Grid level. NERC's explanations of variances, in fact, did not satisfy FERC; the NOPR[xiv] requires yet another set of fixes, as follows:

"The proposed Reliability Standard may, therefore, contain a reliability gap where a responsible entity contracts with a third-party but fails to mitigate potential deficiencies discovered in the third-party's malicious code detection and prevention practices prior to a Transient Cyber Asset being connected to a low impact BES Cyber System. That is because the proposed Reliability Standard does not contain: (1) a requirement for the responsible entity to mitigate any malicious code found during the third-party review(s); or (2) a requirement that the responsible entity take reasonable steps to mitigate the risks of third party malicious code on their systems, if an arrangement cannot be made for the third-party to do so. Without these obligations, we are concerned that responsible entities could, without compliance consequences, simply accept the risk of deficient third-party transient electronic device management practices. Moreover, the requirement to "review" methods used by third-parties to detect and prevent malware may fail to convey the necessary next steps that a responsible entity should take."

In practice, "third parties" (vendors) use of transient devices, or their knowledge of malware in their products, or their dependencies on flawed commercial IT undercarriages, in direct connection to Low Impact Cyber Assets will usually be totally obscure to the "Responsible Entity". Although FERC has approved CIP Standard 003-7, subject to further attention to the perceived flaw above, there are major uncertainties in the protections for Low Impact cyber assets. Note again that less than 10% of Low Impact Cyber Assets are likely categorized as BES Cyber Assets. The flaws, the uncertainties, the proposed fixes may be largely irrelevant for over 90% of BES Transmission Substations. ***FERC should insist that NERC state exactly what BES Transmission systems are covered by CIP Standards and what are not***. The continuous back and forth semantic exchanges between NERC and FERC on security and incident reporting is simply failure to get down to basics, precisely what cyber assets are covered and which are not. What FERC and NERC are fencing about is an appropriate set of semantics that would satisfy security needs while avoiding defining specific protocols that are sorely needed.

5. Low Impact BES Cyber Assets; Incident Reporting

For the mass of BES Transmission substations, it is highly unlikely that utilities have invested in complex ESP systems, and most certainly not expensive EACMS systems at the substation level. In any event, CIP 003-7 is far from precise on intended controls. NERC describes three basic elements involved[xv]:

- ***"Identifying routable protocol communications from outside the asset containing the low impact BES Cyber System*** (at vendors?)
- ***determining necessary inbound and outbound electronic access*** (including secured or unsecured internet connectivity?)
- ***implementing electronic access controls to permit only necessary inbound and outbound electronic access to the low impact BES Cyber System*.**" (between only a vendor and unmanned ICS?)

NERC then expands on the last item, above, i.e., ***"The communication is not used for time-sensitive protection of control functions between electronic devices",*** as stated by NERC, ***"to ensure that the standard does not interfere with control operations."*** How would the vendor know this? What if the contract specifies maintenance support on electronic devices occasionally involved in time-sensitive exchanges?

The foregoing is totally left to the responsible entity. FERC made no apparent effort to parse these limitations/controls in real-world terms, i.e., examples, a limited set of protocols. Precisely what occurs that invokes or negates them? And how do these affect "incident reporting", or if this has any meaning relative to the impact of the incident on the functioning of the BES, or on the Control Center that manages this facility?

What Isologic LLC concludes is at stake here is the widespread practice of vendors (i.e. third parties) connecting directly to ICS systems in Transmission substations, many unmanned, for maintenance of "cyber systems" which, collectively monitor or control OT functions. Thus, vendors are the "third parties" not accountable for malware in their products, thus the absence of standards across a disparate set of systems and vendors and unsecured networks, thus the ambiguous terms/phraseology governing this widespread practice, thus the further FERC charge to NERC in the subject NOPR for consistency in a variety of uncertain environments.

FERC is certainly challenged to get this Internet Connectivity Issue off its back. Under these open-ended uncertainties, there is no, repeat no possibility of reliable "Incident Reporting" from or involving low impact BES (Transmission) facilities. How does an unmanned Transmission substation "report" an incident? FERC must simply accept the fact that the highly decentralized security infrastructures for the BES do not lend themselves to "incident reporting" standards at the Transmission Substation level, that the NOPR on CIP 003-7 of 19 October 2017 is meaningless relative to Incident reporting on Low Impact BES Cyber Assets. Therefore, the current NOPR on Incident Reporting of 21 December 2017 is largely meaningless for Low Impact BES Cyber Assets.

It has taken FERC and NERC almost a decade to dig their organizations into this hole. This industry may have been successful in achieving Grid reliability across 1400 plus independent "responsible entities" but cybersecurity is an entirely different animal. There are in fact, other "third parties", major nation/states that have little difficulty exploiting the vulnerable seams between and among these utilities. In the absence of a Grid-wide security infrastructure, it appears doubtful that any meaningful standards or procedures can be put in place that will even minimally seal off Transmission substations from the nation's adversaries. It should be obvious to all parties that vague CIP objectives, masquerading as "standards" are no protection for the nation's electric system. A minimal cybersecurity infrastructure must be put in place. ***NERC should be tasked to run a deep "red team" review of representative activities between vendors and "low impact Cyber Assets" to firmly establish the facts on security standards, current and necessary, while providing FERC with accurate data on BES Transmission systems not covered by CIP Standards.***

6. Reporting Consistency/Procedures

'There is simply no explanation for the divergence in incident reporting. Security vendors have been reporting widespread adversary activities in the US Grid during 2017. While incidents reported by NERC are consistent with the DOE OE-417 totals, this is only because utilities OE-417 reports satisfy the E-ISAC requirement. However, there is consistent underreporting given the DOE requirement for reporting of incidents that merely have the ***potentia***l for damage[xvi]. Further, the DOE CRISP effort is clearly experiencing many incidents, although their returns are held closely by NERC and DOE. There are also major inconsistencies between the US CERT summaries of incidents involving their forensic services, and those reported by NERC[xvii]. FERC's temporizing on the US CERT numbers (combined electric and water) utilities but clearly largely the former) does not excuse resolution of these conflicts. In 2017, ICS CERT reported a total of 176 in-depth assessments across all sectors, 69%, approximately 120, were from Energy and Water sectors. The vast majority are "demand assessments". This issue is not resolved by this NOPR since FERC itself has been blindsided on the scale of incursions.

NERC should request a DOE IG investigation of violation of DOE regulations implicit in this collusion. FERC staff should routinely monitor incident reporting, authority is clearly provided by the EPA, and this would do no violence to NERC authorities as the ERO.

Further, incident reporting only to the E-ISAC (and ICS-CERT) is wholly insufficient. Incident assessments must be conducted also by the nation's law enforcement authority (e.g., the FBI), by the nation's 24/7 Intelligence Centers, and by responders to attacks (NSA/Cyber Command, Northern Command, State National Guard cyber forces). Utility anonymity can be preserved, when justified. Any incident reflecting serious foreign state adversaries is not "owned" by a utility, or NERC/E-ISAC. If necessary, Congress can be petitioned by FERC to pass necessary legislation that requires the cooperation of utilities in the defense of the nation's critical dependencies on electric power.

Definitions of Cyber Incidents should not be ambiguous. FERC should not proclaim a definition, or associated conditions for reporting, that are inconsistent with DOE OE-417 incident reporting requirements. The OE-417 database should remain the official open source incident database for all utilities. If a classified database is needed, it should be supplemental and cross-referenced to the OE-417 Database. Note there are four OE-417 cybersecurity requirements governing reporting of cybersecurity incidents that have merely the ***potential*** to cause disruption, clearly recognizing the complexity of the nation's adversaries' campaigns involving reconnaissance and intelligence collection.

I respectfully request that the final Rule reflect these conclusions.

III. Major BES and Distribution Vulnerabilities

1. *Fragmentation*

Many issues arise out of the regulatory disconnects in the Nation's power system, notably state and national tariff inconsistencies, oversight of nuclear facilities, accesses and rights-of-way, modernization initiatives, reliability/accessibility to energy sources, interoperability, environmental protections, and or course, operational reliability of the connected mass. Almost every advance and improvement invokes torturous debate and negotiation and frequently interminable delays; occasionally avoidance of critical decisions that must be made. Superimposing cybersecurity atop this fragmented structure through the EPA of 2005, and subsequent legislation has produced a cybersecurity "house-of-cards" known as CIP. It is an attempt at a policy construct, not an operational system.

FERC and the NRC are not responsible for this situation, and there is little they can do to effect change. And admittedly, emergence of nation/state or terrorist threats to the survivability of the nation's electric power have been relatively slow to develop. Nonetheless, each Commission has a responsibility to inform the Congress and the Administration of impediments to reasonable cybersecurity of electric facilities. NRC needs to articulate the dependencies of nuclear generation sites on off-site power sources for safety critical systems. FERC needs to inform Congress of the significant weaknesses in the EPA and the need for a nation-wide, efficient cybersecurity system.

Under the very best of circumstances, the industry is no match for the nation's adversaries. This may have been possible at the time of the EPA, but lost time cannot be made up. ***FERC and the NRC need to support a strong policy of Deterrence as recommended in the DSB report to SecDef***[xviii]***.*** The industry will need at least another decade to build into a "Smart Grid" capabilities (i.e. resiliency) to recover from an attack. Delay is its enemy and need to do this will not vanish.

2. *Systemic Vulnerobilities*

a. *Nation-wide Situational Awareness*

The complete absence of an integrated Grid-wide capability to detect attacks aimed at disabling or capturing a variety of local, regional or national targets represents a vulnerability of staggering proportions. How do Cyber Command and State National Guards respond? ***A structure for real-time situational awareness across both BES and Distribution facilities needs to be created and linked directly to intelligence and other alerting systems both for early warning and for defense of electric and other critical infrastructures.*** The control of this structure can be vested in civil authorities in peacetime but must revert to national security authorities in cyber warfare. This is standard authority transfer in other disciplines (e.g., State National Guards).

Several pieces of such a structure are in place, for example Reliability Regions, the 200+ network of sites coordinating frequency stabilities, the CRISP initiative, networked Synchrophasor sites. For years, the National Synchrophasor Initiative (NASPI) has been working informally in development of standards, data exchanges, application development, and networking of both BES and Distribution facilities (with much progress in the WECC); organized industry cooperation has been lacking, however. ***FERC should require development and institutionalization of a nation-wide Situational Awareness structure; if the FPA is a hindronce, Congress can amend the act.***

b. Communications and Networking

The exclusion from cybersecurity efforts of communications and networks linking so-called Electronic Security Perimeters (ESPs) represents not only a major vulnerability, but also has unintended security consequences across many functional areas. NERC's argument for this exclusion was specious; utilities do not "own" commercial carriers. Neither does DoD but this does not prevent the National Security Community from securing its communications riding on such carriers. The NERC purpose was to avoid having to address complex intra-utility security issues and mutual security requirements across utilities. A plethora of conflicts has emerged; examples: Control Station to Transmission substation communications and Control Center-to-Control Station security. ***Consequently, this exclusion must be eliminated to get utilities to work on cross-enterprise security challenges, there cannot be a Nation-wide integrated network as described above, without removing this CIP 002-5 exclusion.***

c. BES Categorization

The distribution of Cyber Assets into Low, Medium and High categories, based on risks to the BES, miss-categorizes many hundreds of cyber systems relative to threats to the BES overall, and by extension, to the entire U.S. Electric Grid. The issue is particularly acute for so-called Low Impact Cyber Assets. NERC intended this practice to segregate the BES into utility-centric pockets, avoiding the need to address cross-utility cybersecurity issues, or so NERC thought. Permitting each utility to decide to include or exclude a Transmission Substation in coverage by CIP Standards makes hopeless the task of cybersecurity integration for the BES. The practice makes it virtually impossible to operationally integrate cybersecurity for large, regional Transmission organizations such as PJM with 19 major utilities involved. It is, of course, ludicrous for PJM to operationally manage 19 utilities' Transmission systems yet leave operational cybersecurity management in the hands of each utility. Note FERC negotiates Tariffs with PJM, not the separate 19 utilities; but assiduously avoids operational cybersecurity standards which would transcend a utility's boundary. And in its new task, the extension to the Secretary DOE's NOPR, FERC tasks the ISO's and RTO's for comments on cybersecurity resiliency, not individual utilities[xix].

The Nation's adversaries do not approach attack development along utility boundaries, what is seen is much more efficient, focused, exploiting vulnerabilities that are not utility-centric. Consequently, much of the Grid defense suffers from inability to study critical infrastructures and urban targets, their power dependencies reflected in Distribution and Transmission networks and Generation sites, the critical nodes and dependencies involved, defenses in place, or missing. And, of course the attack vectors that would be in play.

This miss-categorization represents lost opportunities for more effective cyber defenses of the entire Grid, not just the BES. As a result, the structure is far more vulnerable than it needs to be.

d. Internet Connectivity

On many of their advisories and alerts, ICS CERT states, relative to Internet dependencies, ***"If you're connected, you're infected"***, and with good reason. Most of their incident studies requested by utilities reveal direct Internet connectivity and associated poor security practices. NERC has been struggling, over the past several years to produce CIP Standards to tighten up Internet-linked security practices involving both control centers and Transmission substations, but without much success. (Earlier discussion in this filing of proposed revisions to CIP 003-7 is but one example.)

The issue is endemic to the industry. Internet scans reveal thousands of direct connections to Cyber Assets (or what should be included as Cyber Assets.) Many Utilities no longer provide trained manpower for technology insertion or maintenance; vendors bundle such services into sales of most major components. Utilities are reluctant to include security requirements in such procurements for fear of increasing costs, and to avoid dependencies which might foreclose shifting to another vendor. ***Note that the proposed CIP Standard 003-7 requirement for "responsible entities" to control transient device connectivity deals with vendor technician physical access to Low Impact Cyber assets but appears to leave wide open vendor remote access across the Internet to such facilities. There is also a long-standing issue involving BES substations that seems to require electronic access (ESP) controls only when: "(3) the communication is not used for time-sensitive protection or control functions between intelligent electronic devices". Does this exclusion apply only to vendor access or does it apply to host remote accesses to Transmission control centers and substations?*** This is further addressed in the Summary and Conclusions in this filing.

Internet connectivity is therefore, a major component of an adversary's attack vectors for phishing expeditions, reconnaissance, malware insertion, intelligence collection and data extraction. Such connectivity is also critical to development of command and control Bots and management of many attacks. IoT DDOS attacks on the electric grid can almost certainly be mounted during more surgical cyber operations. Saturation of call centers in the 2015 Ukraine attack is but one harbinger of future disruptions the Grid might experience.

e. Industrial Control Systems

Perhaps the most neglected segments of Utility cybersecurity controls involve Industrial Control Systems. This is partly due to aging of systems never secured, to the variety of vendor products, to the increasing complexity of substation environments and the absence of systems that can securely manage ICS across substations. But it is also because modernization programs are diffused and frequently lack hard requirements for security, physical or cyber. The very complexity of multiple vendor ICS product mixes has led the international community to develop interface standards, largely communications, to facilitate interoperability. Security is seldom a consideration as these standards have expanded. The Aurora experiments[xx] have demonstrated, conclusively, the damage that can be inflicted remotely on any rotating equipment where electronic access is possible for an adversary

The Synchrophasor (PMU) Map shown earlier in this filing illustrates the increasing complexity of ICS, and their importance. Precision power measurements together with use of GPS timing signals from a subset of such sites permits highly localized power management, certainly good news for power reliability but quite significantly increased the risk of cyber targeting. Security of substations and their ICS has never been more important. However, BES Cyber Standards are applicable only at those sites satisfying Low Impact Cyber Asset Requirements, less than 10% if extrapolations from CIP v4 to CIP v5 are correct. However, all PMU sites (transmission and distribution) are available for cyber attack, those fitting various Russian attack scenarios are of course, unknown. What the Russians undoubtedly know is how to interfere with PMU operations to achieve the purpose of the attack, e.g., Lights Out in Manhattan.

f. Data Flows

Much has changed in the automation of Grid functions, PMUs included. Data feeds to control stations, and therefore to Energy Management Systems (EMS) originate far less often from technicians monitoring sensors feeding SCADA systems and increasingly (and often autonomously) from intelligent ICS. BES Reliability Centers (e.g., PJM's clone, Reliability First Corp) are taking advantage of such data flows for their real-time reliability management functions. Some standardization is occurring, led by International standards-setting bodies, and organizations like NASPI. NERC is clearly playing catch-up but is hemmed in by jurisdictional issues (the BES does not speak for the entire Grid or foreign collaborators.) Cybersecurity is clearly a parallel issue. It was therefore no surprise at a recent NASPI working group meeting to find a recent NERC employee making a pitch for Distribution authorities to voluntarily adopt CIP Standards. None apply to most Transmission PMU substations at this point.

It is therefore fair to ask, how secure are Data Flows from disruption, or worse, manipulation? We know that the data flows from the 200+ sites contributing to the real time AC frequency exchange discussed earlier in this paper are totally insecure. In use of the Internet as a network, these data flows are obviously also open to disruption and manipulation as well. However, we also know that some utilities included security plans in their bids for DOE PMU funding beginning in 2008, which could include encryption of both PMU Data Flows and processing at PMU Data Centers (PDCs). And it is safe to assume that Data Flows at the higher levels of the Grid are secured (Eastern Interconnection Data Sharing Network, for example). However, the integrity of data essential to BES operation, overall, is far from certain, given the complete absence of standards and controls governing this critical resource. In fact, attribution of data source may be very difficult given the unstructured nature of the systems in place, and their use. **This is a major, increasing systemic vulnerability of the electric industry.**

g. Control Center Systems

The major technique used in the Russian takeover of the Ukrainian Distribution Systems, in December 2015[xxi], was phishing attacks for credentials to permit takeover of Control Centers. Ukrainian technicians watched their HMI cursors moving, being controlled remotely from Moscow by Russian operators. The Ukrainian attack tested capabilities to take over HMI functions, to modify ICS systems including firmware, and disable emergency power systems. Actual damage was limited to takeover efforts, no intentional destruction was observed. The earlier 2014 attack on the US Grid apparently involved Supply Chain attacks on Control Center Systems (beginning in 2012) using **Havex** and **BlackEnergy** malware, later seen in the Ukraine. The forensic details of that extended effort in the US Grid were bottled up by DHS, except for industry briefings. However, the ultimate objective of these Russian efforts was to obtain access to ICS systems and associated control systems. And reconnaissance by the same Russian organizations has continued to the present day[xxii].

Following visits by DHS and other US authorities, the Ukraine government publicly clammed up on attribution of these events to the Russian Government. NERC is quite witting of this string of incidents while publicly denying their associations, and downplaying the potential impact on Grid reliability. It has been left to security firms, domestic and abroad, to draw the associations and to document attribution to the Russian Government. A good deal of the information on specific flaws in control systems has been documented by security firms. With great care to avoid citing Russia as the perpetrator of all this, ICS CERT has been forced to put the forensics in the public's hands and in fact, to provide Yara tools for detection, (incident reporting, hopefully) and removal. **What game was DHS playing in these machinations?**

We now understand that Russia has stealthy capabilities to access and modify control systems at the vendor facility. We also know that they have skilled personnel to capture control of these systems at utilities. With these tools unquestionably in the hands of experienced Russian personnel, there is little to prevent a takedown of major US electric facilities, through control system vulnerabilities. Ineffective security controls at so-called ESPs or EACMSs have apparently done little to prevent targeted Russian reconnaissance and intelligence collection in the US. **In suppressing the reporting of these incidents, what game is DoE and NERC playing?**

h. Supply Chains

The security integrity of industry products is, today, highly suspect. Flaws in development and production of vendor-unique systems often escape notice until they show up in cyber exploitation efforts. The recent disclosure of **Meltdown**[xxiii] and ***Spectrum***, CPU architectural flaws, shows clearly that systemic vulnerabilities can exist for many years, undetected (but may have been known to nation/states).

Foreign adversaries have many ways to penetrate Supply Chains, down to the HW electronic component level, and more easily in Software updates, if this cannot be done at vendor's plants. Testing by utilities would be impossibly costly. CIP Standards as drafted require utilities to develop defenses, but that guidance would specifically enjoin utilities from putting pressure on vendors. This is questionable guidance; how else to leverage vendors to test their products, and control access in the Supply Chain. Whitelisting and Blacklisting would quickly turn this situation around. ***(Q)*** Why hasn't this occurred? ***(A)*** Because the industry does not take this vulnerability seriously.

The issue is compounded with the vendor practice of developing utility-unique systems to ride atop commercial information technologies, e.g., Windows OS, Linux OS, commercial data base systems, including networking systems[xxiv]. It is common practice for IT vendors to expect users to find difficult flaws; in the hands of cyber offense experts, these constitute "zero-day vulnerabilities". The nation's adversaries are quite adept at finding and exploiting such IT flaws. Many of the exploits seen today ride on commercial IT flaws.

Correcting or offsetting Supply Chain vulnerabilities is one of the most significant challenges to Utilities. It is so difficult that it must be shared by the federal government. The recently announced Vulnerability Equities Policy (VEP) guidance is a starting point since it covers revelation of vulnerabilities, with exceptions that are critical to the national security. Industry-wide testing of major systems should be instigated with whitelisting of "good" products. In short, there is no escaping the need for a comprehensive program to address the issue.

3. Summary

The vulnerabilities outlined above are fundamental, indeed "systemic". By design, there is little that the Industry and NERC can or will do to assuage real risks to the BES within the cybersecurity agenda with policy-level Critical Infrastructure Protection Standards. This coalition has successfully hunkered down behind (1) the absence of a damaging Grid attacks (2) general and non-specific CIP requirements, (3) deception, and controlled suppression, of Russian incursions, reconnaissance, and collection efforts over recent years, and (4) a "frozen-in-place" national leadership that has been largely in denial of the threat. There has been no serious effort to ensure compliance of admittedly, inconsequential CIPs, with consistent attempts by NERC to water down reporting requirements and put any assessment of compliance under "no-public-release" wraps[xxv].

IV. Threats

Historians have a way of looking back on important events, identifying flash points in national security affairs that were minimized at the time. Will the decade-long failure to evaluate the growing risk to the nation of a highly-vulnerable National Grid (nuclear, distribution, transmission systems) be similarly assessed in years to come? Or will this evolution fall into the same category as the "missile gap" of the 50s and 60s? Time will tell. Threats do matter, particularly when viewed against a backdrop of vulnerabilities. Pearl Harbor was a tragedy but a major vulnerability was not present, the US carriers were elsewhere. So pure luck does count, and perhaps the nation will eventually put a cyber deterrence policy in place while developing a resilient, recoverable Smart Grid. Time will tell. At present, it is important in this filing to assess existing threats in the hope that regulatory commissions, FERC and the NRC, make more prudent cybersecurity decisions considering the major unknowns of cybersecurity policy.

1. Russia

A substantial offensive cyber capability has been achieved by Russia. It is clearly a component of an aggressive national Information Operations campaign that has kept the United States off-balance in two Administrations. The principal organizations are the FSB and the MOD/GRU, the latter of increasing prominence in actions such as the hacking of the DNC and a robust presence in the election activities of 21 states[xxvi]. Since 2014, the Russian agenda appears to favor the GRU, probably reflecting a leadership decision to press substantial military intelligence manpower into cyber-intensive areas. Occasional incidents in European Energy networks are also being reported. The GRU has been active in Syria, including apparently training the Syrian Electronic Army, which was in turn, largely responsible for the fall of Aleppo to the Syrian regime. There are also reports of the GRU active in the Eastern Ukraine, probably behind the subversion of Ukrainian military artillery battlefield software. This suggests that GRU teams are being trained for specific missions. However, incident attribution to either the FSB (APT 28) or GRU (APT 29) is not always certain; several security firms and Federal agencies avoid attribution entirely[xxvii]. However, it appears that the GRU has assumed the main responsibility for targeting Energy Grids.

a. The Grid Campaign to-date

In 2014 there was a major incursion into the US Grid[xxviii], employing malware that traced to earlier use by probable Russian criminal elements. Its use by the GRU followed penetration through Supply Chain vulnerabilities. A 2015 takedown of Ukraine Electric Distribution facilities involved a different penetration strategy but with an upgrade to the same malware; therefore, it was probably the GRU. The attack was mounted remotely from Russia, according to Ukraine authorities, but was not intended to damage facilities. A year later, in December 2016, an attack attributed to Russia took down a Transmission facility for one hour, probably a demonstration believed to be a strong signal to President Obama to resist cyber retaliation for the DNC hack. The message was apparently received. Cyber penetrations in the US Grid continued throughout and into 2017, reported by ICS CERT[xxix]:

Comment: The referenced Alert contains extensive documentation by several security firms of Russian incursions into US/Canadian (and some foreign) energy networks, continuing from 2015 and throughout 2017. ICS CERT makes no attempt to sort through the variety of actor/malware covernames but there is no disguising the perpetrators as APT 29/GRU. This alone is critical since it involves Russian military Cyber elements whose crisis role is unquestionably cyber attack. Further these reports suggest that tactics have shifted from pure reconnaissance to attack development. The Putin Cyber strategy has been effective; US policy is totally stalled. What is worrisome is the possibility of miscalculation; what controls are in place to keep a GRU team from disabling a major US facility? The comprehensive industry analysis reflected in the ICS CERT Alert proves that DoE OE-417 rules on cyber incident reporting are being flagrantly violated by the Industry and NERC and ignored by regulatory authorities. It should be further noted that the Alert provides substantial technical content that would permit many utilities to identify and mitigate/remove malware from their cyber systems. Little further evidence is needed to confirm the existence of a massive industry/regulatory coverup of Russian offensive Cyber efforts against the North American Grid.

a. Attack Technologies and Techniques

Russian tools observed to date have shown increasing sophistication, redundancy, stealth, and lethality, with apparent good knowledge of vendor security flaws. They do not fear discovery, or even attribution, counting on the Russian tactic of plausible deniability and the willingness of agencies and national administrations to deny attribution. Modification of vendor products (at the vendor), exploitation of control system weaknesses in control centers, remote replacement of firmware in ICS devices has been experienced, expropriation of third party servers for BOT purposes is common. Their reconnaissance malware ***(HAVEX)*** works with several "dropper" techniques, generally bypassing security control in targeted systems, capable of undetected penetration of Grid IT, embedding a back door in the system, communicating with the attacker's command and control systems, and moving laterally through networks collecting infrastructure details (to be reported back to attack controllers). The disabling malware ***(BlackEnergy)*** is stored on command and control servers until needed. In the brief takedown of a Ukraine Transmission system, a new malware package was recovered, named ***Industroyer***[xxx] by its discoverer, ESET. It exploits a widely-used international communications interface standard, ***IEC 61850*** with malware add-ons that were tailored to Ukrainian ICS for testing and can be modified and used extensively in the US Grid, for ICS capture and/or destruction. The

Russian undoubtedly understand the value of this attack vector given the absurdity of excluding communications and networks from CIP Standards.

It is quite common in Russian attack systems to exploit standard commercial information technologies, operating systems, networking systems, commercial data bases, exploiting flaws in such systems. They are aware of "zero-day" security issues in energy-associated IT systems, for example in the 2014 incursions into the US Grid, they exploited one such operating system security weakness to gain entry to three different control systems used by utilities[xxxi]. OT vendors often have no choice but to mount their utility-specific systems aboard standard commercial IT, generally unaware or indifferent to the vulnerabilities of such systems. Upgrading or replacing commercial IT is generally left to IT vendors, e.g., Patch Tuesday for Microsoft. Obtaining user credentials is often the main penetration vector through phishing techniques. During the Ukraine incursions in 2015, the GRU mounted a Denial of Service (DOS) campaign from Moscow, essentially obliterating a call center to sow confusion through the Utility and of course, preventing call-in by its blacked-out clients. Russia experimention with new attack systems (***FURTIM***, earlier described, are occasionally detected. ***Industroyer***, and a version of ***WannaCry*** (for DDOS, not fundraising goals) cautious of course to limit exposure to Western forensic eyes. Until Russia achieves a high level of attack automation, targeting will be limited and largely the job of the GRU, which is what is observed. CIP Standards consistently fail to protect utilities until a "heads-up" heralds the identification of incursions.

2. China, North Korea and other Nation States

The question often arises, "what other countries are a threat to the Nation's electric system?". China has been pressured to cease their industrial espionage efforts in the US, largely in Defense Industry foraging. Reports from US security firms state that this has fallen off considerably[xxxii]. There are dated reports of probable Chinese cyber efforts directed against West Coast and Canadian energy targets, likely technical intelligence collection. The main Chinese cyber threat is from the Ministry of State Security which has maintained a very stealthy presence across international networks for years. Collaborating US IT and Security Firms have labelled its activities, ***Axiom***[xxxiii], which closely parallel Chinese government interests, world-wide. Targeting of energy firms will of course be kept well hidden.

North Korea's cyber operation, known as ***Hidden Cobra***[xxxiv] has been in existence since at least 2006. Its capabilities include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. RATs are full-function malware capable of infecting victim systems for persistent espionage or destructive activities, run remotely from C + C servers. Recently, the Administration announced a successful effort to disable NK WannaCry operations that were targeting over 250,000 victims. The NK effort was likely aimed at collecting badly needed foreign currencies through victim intimidation. NK Cyber Warfare planning would almost certainly include US Grid destructive efforts although these have not been observed in ***Hidden Cobra*** incursions in the U.S. DHS and the FBI are intensifying their reporting of NK cyber threats[xxxv]. Major targets are Communications and Financial institutions.

The main terrorist threat to the US Grid would likely come from nation/state cyber-trained individuals or small groups recruited from cadres such as the Syrian Electronic Army or domestic recruits from US IT fields. It is truly surprising that such an effort has not yet been experienced by a U.S. Utility (or perhaps it has been and failed to make it into the public-facing incident database.)

3. *Regulators' Awareness*

It is difficult to keep up with all the threat information circulating in open media. In this regard, the nation suffers from permissive, competitive, unregulated IT and Security industries, most doing business abroad. Fortunately, major clients including federal agencies generate serious requirements for defense of their organizations and IT systems and knowledgeable analysts can track major threats. The most important threats to the North American Grid have been captured in Isologic's "Security in the North American Grid" White Papers, copies of which are routinely sent to both FERC and the NRC. The technical Staffs at Regulators really ought to be current on threats and be encouraged to routinely advise Commissioners on threats. Or competent security firms ought to be under contract to provide independent assessments, and linkages to intelligence centers ought to be in place to provide classified threat information. It is truly worrisome that FERC does not weigh threats in its cybersecurity rule-making role for the North American Grid.

V. Summary and Conclusions

This filing contains specific comments and recommendations on the NOPR [Docket Nos. RM18-2-000 and AD17-9-000] Cyber Security Incident Reporting Reliability Standards, Issued December 21, 2017. It also contains late comments on NOPR [Docket No. RM17-11-000] Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls, Issued October 19, 2017. The latter is a classic example of band-aid patches to earlier band-aid patches and eventually to existential flaws. Back to Order 791 and all that follows on security of communications including Internet connectivity to/from low-impact cyber assets. It is virtually impossible to track changes. Transmission stations and substations included or excluded from CIP cyber asset categorization is deliberately obscured. Utilities have the option of labeling the entire facility as a "cyber asset" (if it is meets CIP 002-5.1 criteria) so where is the clarity on any-and-all cybersecurity issues? It must be impossible for compliance auditors to understand these requirements, end-to-end. ***More importantly, FERC needs to explain in the final rule on incident reporting what the mandatory requirements are for utilities to report cyber incidents.***

This filing also contains much additional information and recommendations on Vulnerabilities and Threats in order that the Commission understand its profound obligation to protect the public, its institutions, dependent Critical Infrastructures, and the Nation's security when it states: ***"the proposed CIP Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest".***

Critical Information Protection (CIP) Standards as they exist today are hardly more than high level policy "objectives" that completely lack substantive content and protocols, and absent a nation-wide cybersecurity infrastructure, fail to protect the nation's Bulk Electric System (BES) from disruption or destruction by the nation's adversaries. CIP Standards are an extremely poor adjunct to other Reliability Standards essential to functioning of the BES. Even if the nation had a strong Deterrence Policy in place, risk from all quarters cannot be eliminated. No one expects that a commerciallyfragmented and minimally-regulated electric industry can protect itself, or ever achieve a degree of resiliency to survive a determined nation/state attacker. What is feasible is that a cybersecurity infrastructure across electric utilities (including Distribution assets) be put in place, a reasonable situational awareness program be established nation-wide, and realistic security standards and procedures be developed and enforced. Any complaint that the EPA does not authorize FERC to take the lead on protecting the nation rings hollow if the Commission fails to make the following needs known to the Congress:

- ***eliminate all exclusions from CIP Standards,***
- ***correct the fundamental error on "communications networks" vs. ESPs,***
- ***task DOE to organize a nation-wide situational awareness structure building on CRISP and emerging PMU networks,***
- ***use of encryption on all internet operational connectivity including vendor maintenance,***
- ***remove known malware from utility systems when feasible,***
- ***whitelisting and blacklisting for all vendor systems known to be targeted by adversaries,***
- ***collaborate with states on training, and use of National Guard elements for mitigation of incursions/attacks,***
- ***ensure incident reports go to all Federal agencies involved in Cybersecurity matters,***
- ***support the DoD Science Board recommendations on Deterrence Policy,***
- ***petition Congress to authorize recovery of cybersecurity costs in tariffs.***

Finally, addressing the threat to the nation on loss of a major segment of the electrical system, it is surreal that Russian presence in the North American Grid would be tolerated by the industry and its regulators and kept from the public. It is equally surreal that the Commission cannot issue a simple, unequivocal order that known malware will be removed from the BES OT and IT systems.

Respectfully Submitted by:

George R. Cotter

George R. Cotter
grcotter@comcast.net
Isologic, LLC
183 Southdown Rd
Edgewater, MD 21037

Endnotes

[i] **OE-417 ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT, DoE, Nov 2014**

[ii] **NERC's June 30, 2011 response to FERC's April 12 2011 data call**

[iii] **"lights Out", Ted Koppel 2015**

[iv] **"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. Foundation for Resilient Societies**

[v] **G.R. Cotter, "Security in the North American Grid, A Nation under Siege" A White Paper, September 30, 2016**

[vi]See, for example: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01E

[vii] Docket No. RM16-18-000, Cyber Systems in Control Centers, (Issued July 21, 2017)

[viii] See for example, "Why Linux is better than Windows or macOS for security", By Dave Taylor Computerworld | Feb 6, 2018 3:31 AM PT 16)

[ix] NIST SP 800-16, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015

[x] "How to remove malware from your Windows PC" PC World Oct 15, 2017

[xi] Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000 AD17-9-000 21 Dec 2017, para 17

[xii]See, for example: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01E

[xiii] See Para 36, NOPR RM18-2-000, AD17-9-000 21 Dec 2017

[xiv] See Para 4, NOPR RM18-2-000, AD17-9-000 21 Dec 2017

[xv] Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls Docket No. RM17-11-000 Oct 19 2017

[xvi] OE-417 ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT, DoE, Nov 2014

[xvii] ICS-CERT-Monitor Report, Nov-Dec 2017

[xviii]Department of Defense, Defense Science Board, Task Force on Cyber Deterrence, February 2017

[xix] FERC ORDER TERMINATING RULEMAKING PROCEEDING, INITIATING NEW PROCEEDING, AND ESTABLISHING ADDITIONAL PROCEDURES AD18-7-00 (Issued January 8, 2018)

[xx] What You Need to Know (and Don't) About the AURORA Vulnerability 09/01/2013 POWER Joe Weiss et al.

[xxi] Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, SANS ICS/E-ISAC Report March 18, 2016

[xxii] TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors 10/20/2017 06:50 PM EDT

[xxiii] Protecting your device against chip-related security vulnerabilities, Microsoft Support, Jan 2017

[xxiv] G.R. Cotter, Security in the North American Grid, Supply Chain Vulnerabilities and Threats, A White Paper, Mar 2017

[xxv]NERC Docket No. RR15-2-000, Annual CMEP Filing. Latest example of NERC efforts to deny public access to compliance failures.

[xxvi] DHS officials: 21 states potentially targeted by Russia hackers pre-election, By Tal Kopan, CNN

[xxvii] Dragonfly: Western energy sector targeted by sophisticated attack group, Symantec (Note: Dragonfly is Russian)

[xxviii] Alert (ICS-ALERT-14-176-02A ICS Focused Malware (Update A) Last revised: July 01, 2014

[xxix] Alert (TA17-293A), Last revised: October 23, 2017

[xxx] Industroyer: ICS protocols were developed decades ago with no security in mind, ESET, 19 Jun 2017 - 11:00AM

[xxxi] ICS CERT Alert (ICS-ALERT-14-176-02A

[xxxii] FIREEYE iSIGHT INTELLIGENCE, CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE REDLINE DRAWN, June 2016

[xxxiii] FIREBALL – The Chinese Malware of 250 Million Computers Infected by Check Point Threat Intelligence Research Team posted 2017/06/01

[xxxiv] Alert (TA17-164A) HIDDEN COBRA – North Korea's DDoS Botnet InfrastructureLast revised: August 23, 2017

[xxxv] White House officially blames North Korea for massive 'WannaCry' cyberattack December 19, 2017

Febuary 25, 2018

Chairman Kevin J McIntyre

Commissioner Neil Chatterjee

Commissioner Cheryl A LaFleur

Commissioner Robert F Powelson

Commissioner Richard Glick

Federal Energy Regulatory Commission

888 First Street, NE

Washington, DC 20426

Comments submitted in FERC AD17-9, Cyber Security Incident Reporting Reliability Standards

Dear Chairman McIntyre, Commissioner LaFleur, Commissioner Chatterjee, Commissioner Powelson and Commissioner Glick:

These comments are being submitted by Qui Tam Analytics to enlighten the Federal Energy Regulatory Commission (FERC) to encourage the North American Reliability Corporation (NERC) to mitigate, log, and remove any and all malware from the "Bulk Electrical System" Grid by setting enhanced standards for malware detection, reporting, mitigation and removal. It is also being submitted to encourage both to begin an immediate assessment of the overall Electrical Grid by third party subject matter experts to evaluate already exploited areas within the Grid which may have embedded malware and report those findings to the public.

Malware reporting structures within NERC/FERC have caused alarm to the public.

Qui Tam Analytics, and many organization within the cyber security community are questioning the current reporting structure as to the accuracy of Grid malware intrusions, the metrics of those intrusions, the corrective actions taken by NERC necessary to mitigate them in a timely fashion, the exploits themselves and the level of facilities that are actually being compromised. Patterns in historical data would indicate that the Bulk Electrical System and its current exposure to malware is being under reported by NERC, due to their method of determining the malware exploit's damage after a disruptive event has taken place instead of mitigating the exploit prior to its triggering timetable.

Malware isn't a fallen tree branch, that has breached a power line during a thunderstorm. It's an evasive malignant tumor waiting for the right moment to attack and kill the body, the Bulk Electrical System.

FERC's New definition of "Bright Line" thresholds including most facilities and their definition associated with Bright Line, operating above or even below 100kv are giving pause to even the casual observer. FERC requirements and Critical Infrastructure Protection (CIP) reliability standards associated with malware exploits are truly unacceptable, at this point in 2018.

Patterns of exclusions, exceptions, variances and self determinations by investors, public utilities, transmission partners or local distribution facilities of those commodities are becoming more and more problematic.

Although the Commission claims it is using the 7 factors test developed previously in order No 888, FERC seems to vary their determination of facility level risk based on a sliding scale and case by case core definitional variances of BES facilities.

Exception processes where 150kv definition are the threshold one moment, 200kv or even 500kv, at others, takes away the seriousness of defining the exact consistent variables that are necessary for (CIP) standards to determine compliance.

From a predictive analytics standpoint of view, this lack of continuity caused by exceptions in the BES standards makes it harder to pin point the relative data points and indicators that could be used to evaluate step-wise logistic regression models and do analytics on the possible vulnerable facilities, assets or malware entry points. It also makes any use case formulation and evaluation of the relevant data harder to model because the data isn't consistent and indicators vary. It does little for malware resolution if you can't gather the indicators necessary to develop a model.

A baseline approach would be to assume that there are corrective actions needed presently to avoid getting blindsided by a malware attack.

Malicious malware intrusions by adversaries within the BES, will be inevitable, if planning and malware specific CIP reliability Standards aren't done to mitigate those intrusions. Adversaries may not care what facility or asset the malware gets imbedded, they only care where it can be easily embedded to be to do the most damage. It may be lurking in a local distribution facility waiting to worm its way to other BES facilities. If the facility is in a more rural area, it may be an easier target to imbed the malware through a media USB injection. Facilities that are associated with a larger public utilities usually have server side or network administrators or engineers running their Information Technology departments. Those staff members have server administration authorization rights to eliminate uploads that may be malware related but still can be embedded through backdoor methods. Smaller substations and rural facilities have to worry about both scenarios.

Indirect or direct, up or down stream BES trivializing about facility core definitions only compounds malware exploits that may be dormant currently. Non reporting, skewing the number of exploits, and not removing malware only increases the concern for BES malware intrusions.

Those embedded exploits may be waiting for a triggering event in a facility that was defined differently than the core BES definition and in which the Commission determined was less of a problematic facility for BES purposes . Those cascading malware exploits will become exponentially problematic based on the incorrect "Bright Line" evaluations of those facilities.

Critical Infrastructure Protection (CIP), Standards should detect, report and remove those malware intrusions before a triggering event causes harm. Standards must have a hard line definition to circumvent these Bulk Power System Malware threats which would cause Electrical Grid Failure.

Having a voluntary participation program such as the CyberSecurity Risk Information Sharing Program(CRISP) does little good if they are voluntary. A non active member facility may be the facility that creates the impetus to take down the BES.

Inaction by FERC of malware exploits based on section 215 of the Federal Power Act is unacceptable, as well, because malware can be configured to worm its way through to a "one infected, all infected" stage, making specific excluded categories and facility networks the spring board for the intrusions.

If the facility is online, with the internet, it is vulnerable to malware and is within the Commissions legal jurisdictional control, even if it is a local distribution facility. Malware communication can reach all platforms, and thus, would be categorized as a BES event which would authorize FERC to remedy the problem.

This sections comments are to advise NERC and FERC the seriousness of the malware problem within the Bulk Power System and that it can no longer be marginalized. It advises them that the general public is concerned and aware of its dangers. It recognizes that the casual observer perceives the Commissions inaction in regards to malware vulnerabilities, reporting, and removal within Bulk Electrical Grid structure, it's cyber security solutions, it's Critical Infrastructure Protection and those malware exploits to the Bulk Power System.

CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations was created by DRAGOS, INC. They are highly recognized cyber security subject matter experts who have been involved with the observation of electrical Grid vulnerabilities and exploits. They are currently following Electrum the group that is believed to have caused the Ukrainian Power Grid failure. They have no association with Qui Tam Analytics, this comment, its submittal or any affiliated companies. They are an excellent resource of individuals who have a plethora of Intelligence Community backgrounds. Their working papers have been extremely helpful to this author.

They are Important and informative.[1] Excerpts of their work product, which is submitted here, deserve more than a mere foot note and their advice that "Adversaries are getting smarter, they are growing in their ability to learn industrial processes and codify and scale that knowledge, and defenders must also adapt."

The following are excerpts from CRASHOVERRIDE by DRAGOS, Inc

Ukraine Cyber Attack 2015

The cyber-attack on three power companies in Ukraine on December 23rd, 2015 marked a revolutionary event for electric grid operators. It was the first known instance where a cyber-attack had disrupted electric grid operations. The Sandworm team was attributed to the attack and their use of the BLACKENERGY 3 malware. BLACKENERGY 3 does not contain ICS components in the way that BLACKENERGY 2 did. Instead, the adversaries leveraged the BLACKENERGY 3 malware to gain access to the corporate networks of the power companies and then pivot into the SCADA networks. While in the environment the adversaries performed their reconnaissance and eventually leveraged the grids systems against itself. They learned the operations and used the legitimate functionality of distribution management systems to disconnect substations from the grid leaving 225,000+ customers without power for upwards of 6 hours until manual operations could restore power. However, due to the wiping of Windows systems through the KillDisk malware and destruction of serial-to-Ethernet devices through malicious firmware updates, the Ukrainian grid operators were without their SCADA environment, meaning they lost the ability for automated control, for upwards of a year in some locations. The most notable aspect of the attack was the adversary’s focus on learning how to leverage the systems against themselves. Malware enabled the attack, and malware delayed restoration efforts, but it was the direct interaction of the adversary leveraging the ICS against itself that resulted in the electric power disruptions, not malware.

CRASHOVERRIDE

The CRASHOVERRIDE malware impacted a single transmission level substation in Ukraine on December 17th, 2016. Many elements of the attack appear to have been more of a proof of concept than what was fully capable in the malware. The most important thing to understand though from the evolution of tradecraft is the codification and scalability in the malware towards what has been learned through past attacks. The malware took an approach to understand and codify the knowledge of the industrial process to disrupt operations as STUXNET did. It leveraged the OPC protocol to help it map the environment and select its targets similar to HAVEX. It targeted the libraries and configuration files of HMIs to understand the environment further and leveraged HMIs to connect to Internet-connected locations when possible as

[1] CRASHOVERRIDE Analysis of the Threat to the Electric Grid Operations is the Work Product of DRAGOS, Inc./WWW.DRAGOS.COM 1745 Dorsey Rd. Hanover, Maryland 21076

BLACKENERGY 2 had done. And it took the same type of approach to understanding grid operations and leveraging the systems against themselves displayed in Ukraine 2015's attack. It did all of these things with added sophistication in each category giving the adversaries a platform to conduct attacks against grid operations systems in various environments and not confined to work only on specific vendor platforms. It marks an advancement in capability by adversaries who intend to disrupt operations and poses a challenge for defenders who look to patching systems as a primary defense, using anti-malware tools to spot specific samples, and relying upon a strong perimeter or air-gapped network as a silver-bullet solution. Adversaries are getting smarter, they are growing in their ability to learn industrial processes and codify and scale that knowledge, and defenders must also adapt.[2]

Qui Tam Analytics is requesting that FERC take heed to that advice, and consistent with Commission authority for electric reliability under Section 215 of the Federal Powers act. We ask the Federal Energy Regulatory Commission ("FERC" or "Commission") to order the North American Electric Reliability Corporation ("NERC") to set an enhanced standard for malware detection, reporting, mitigation, and removal ("Malware Standard")

Respectfully Submitted,

Jerry Ladd
Qui Tam Analytics

[2] Thank you Rob at DRAGOS for allowing Qui Tam Analytics to use excerpts of your work product for the Greater Good of the BES

Document Content(s)