UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Foundation for Resilient Societies	**)**	**Docket No. AD17-9-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN OPPOSITION TO PETITION FOR RULEMAKING

The North American Electric Reliability Corporation ("NERC") hereby provides comments in opposition to the Foundation for Resilient Societies ("Resilient Societies") Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk-Power System ("the Petition"), filed with the Federal Energy Regulatory Commission ("Commission") under Rule 207 of the Commission's Rules of Practice and Procedure in the above-captioned docket.[1] The Petition requests that the Commission direct NERC to develop a Reliability Standard that would require Responsible Entities[2] to detect, report, mitigate, and remove malware that could affect BES Cyber Systems and file the Reliability Standard within 90 days of the order directing development.[3]

NERC respectfully requests the Commission deny the Petition. NERC appreciates the risk that malware poses to the Bulk-Power System ("BPS") and uses its many reliability tools to mitigate this risk. As discussed below, NERC's enforceable Reliability Standards, current standard development activity, and other cyber security efforts adequately address the threats, vulnerabilities, and risks associated with malware detailed in the Petition. A new Reliability

---

1 *The Commission's Rules of Practice and Procedure,* 18 C.F.R. § 385.207(a).

2 The Critical Infrastructure Protection 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 *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) at p. 2.

Standard to address malware detection, reporting, mitigation, and removal is thus not necessary at this time.

NERC's currently enforceable suite of Critical Infrastructure Protection ("CIP") Reliability Standards employ a risk-based approach to Bulk Electric System ("BES") cyber security and mandate controls commensurate to the risk posed by threats and vulnerabilities to the reliable operation of the BES. Several of the Requirements within the CIP Reliability Standards require Responsible Entities to implement protections from the threat of malware. As with all of its standards, NERC continually evaluates whether additional protections are needed as it reviews the manner in which entities implement the required controls and the effectiveness of those controls.

Pursuant to Order Nos. 822 and 829, NERC is currently developing modifications to its CIP Reliability Standards that further enhance protections that mitigate the risks of malware.[4] Specifically, under Order No. 822, the Commission directed NERC to modify the CIP Reliability Standards to include additional protections for communications links and sensitive BES data communicated between BES Control Centers and to enhance protections for low impact BES Cyber Systems.[5] In Order No. 829, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations.[6] These ongoing development activities seek to strengthen the cyber security controls included in the CIP Reliability Standards and specifically target the threat of malware, as discussed below. Therefore, NERC's currently enforceable CIP Reliability Standards and ongoing development efforts address issues

[4] Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, 81 Fed. Reg. 4177 at paras. 3, 18, 64 (2016) ("Order No. 822"); Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 FERC ¶ 61,050, 81 Fed. Reg. 49,878 (2016) ("Order No. 829").

[5] Order No. 822 at para. 3.

[6] Order No. 829 at para. 1.

identified in the Petition, and the Commission does not need to direct NERC to revise the CIP Reliability Standards as requested in the Petition.

The Commission is currently reviewing the CIP Reliability Standards to determine whether additional modifications may be needed to address, among other things, risks associated with malware. Specifically, the Commission issued a Notice of Inquiry ("the NOI") seeking comment on the need for, and the possible effects of, modifications regarding "(1) separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions; and (2) computer administration practices that prevent unauthorized programs from running, referred to as 'application whitelisting,' for cyber systems in Control Centers."[7] The Commission's review, coupled with NERC's continuous review of its Reliability Standards, should identify further revisions, if necessary, to the CIP Reliability Standards. Thus, the Commission should not direct NERC to develop Reliability Standards as outlined in the Petition prior to completing this review.

While NERC's CIP Reliability Standards provide the foundation for cyber security practices in the electric subsector, NERC's efforts to achieve effective cyber security extend beyond enforcement of mandatory Reliability Standards to enhancing industry's situational awareness, real-time communication, and prompt emergency response capabilities.[8] NERC operates the Electricity Information Sharing and Analysis Center ("E-ISAC"), which is a key component in providing these capabilities for the electric sector.[9] Among other things, E-ISAC collaborates with the Department of Energy ("DOE") on the Cybersecurity Risk Information Sharing Program, which provides timely, bi-

---

[7] Notice of Inquiry, *Cyber Systems in Control Centers*, 156 FERC ¶ 61,051, 81 Fed. Reg. 49,641 (2016) at 2.

[8] *The Electricity Sector's Efforts to Respond to Cybersecurity Threats: Hearing before the Subcomm. On Energy of the H. Comm. On Energy and Commerce*, 115th Cong. § 5 (2017) (statement of Gerry W. Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation), *available at* http://docs.house.gov/meetings/IF/IF03/20170201/105497/HHRG-115-IF03-Wstate-CauleyG-20170201.pdf.

[9] *Id.*

directional sharing of unclassified and classified threat information.[10] Moreover, NERC uses an alert system, called NERC Alerts, to communicate unclassified, sensitive information to industry and recommend entities take certain action to enhance their cyber security posture.[11] Since 2009, NERC has issued 41 cyber-related alerts, including an alert regarding the cyber security event in Ukraine in 2015.[12] NERC and industry also engage in security exercises that simulate crisis scenarios and allow industry to test incident response procedures. These security tools complement NERC's mandatory Reliability Standards to mitigate the cyber security risks to the electricity sector. Because these activities effectively address some of the concerns detailed in the Petition, the Commission should not direct NERC to incorporate them into mandatory Reliability Standards.

These comments are organized into three sections. Section I.A discusses the currently enforceable CIP Reliability Standards and their protections from malware. Section I.B provides an update on current standards development activities that address enhancements to the existing Reliability Standards. Finally, Section I.C highlights NERC's other cyber security activities that do not involve mandatory Reliability Standards.

I. COMMENTS

A. NERC currently has enforceable Reliability Standards that address cyber security threats from malware to the Bulk-Power System.

In the Petition, Resilient Societies notes that assets of the BPS are exposed to malware threats because the assets are connected to the public internet.[13] Resilient Societies further asserts cyber attackers can use implanted malware to steal passwords, conduct reconnaissance, extract data, remotely execute grid control, cause blackouts, and destroy equipment.[14]

---

10 *Id.* at 7.
11 *Id.* at 8.
12 *Id.* at 8-9.
13 Petition at 2.
14 *Id.*

As NERC commented in response to the NOI, the currently enforceable CIP Reliability Standards include a number of Requirements designed to mitigate the risks associated with Internet connectivity.[15] These Requirements mandate controls to mitigate the risks of remote access through the Internet, reduce the attack surface of Cyber Assets, help ensure Responsible Entities fix known software vulnerabilities that could be exploited by a malicious actor through the Internet, and help prevent and mitigate the threat of malicious code that may be introduced through Internet connections.[16] NERC and industry designed the currently enforceable CIP Reliability Standards to address the risk of malware detailed in the Petition. Therefore, NERC has current protections in place to mitigate the threat of malware to assets of the BPS.

Specifically, as detailed in the NOI Comments, the CIP Reliability Standards include several Requirements that address the risks associated with malware, including:

- *CIP-005-5, Requirement R1* requires entities to establish an Electronic Security Perimeter ("ESP") to control electronic access to BES Cyber Systems. An ESP is the "logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." Among other things, Requirement R1 specifies that (1) all External Routable Connectivity, such as Internet connections, must go through an Electronic Access Point ("EAP") that requires inbound and outbound access permissions based on a valid need for granting such access; and (2) each EAP has one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

- *CIP-005-5, Requirement R2* addresses the protections required for Interactive Remote Access, which is defined as "[u]ser access by a person employing a remote access client or other remote access technology using a routable protocol." Requirement R2 mitigates the risks of remote access through the Internet by requiring that entities (1) use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset; (2) use encryption that terminates at an Intermediate System; and (3) require multi-factor authentication for all Interactive Remote Access sessions. These remote access protections would significantly impair a malicious actor's attempts to perpetrate the type of cyberattack carried out in Ukraine referenced in the NOI.

---

[15] *Comments of the North American Electric Reliability Corporation in Response to Notice of Inquiry*, Docket No. RM16-18-000, at 5 (filed Sep. 26, 2016) ("NOI Comments").

[16] *See* NOI Comments at 5.

- *CIP-007-6, Requirement R1* requires entities to (1) enable only logical network accessible ports that have been determined to be needed by the Responsible Entity; and (2) protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. The controls help reduce the attack surface of Cyber Assets.

- *CIP-007-6, Requirement R2* requires entities to implement a patch management process for tracking, evaluating, and installing cybersecurity patches. This security control helps ensure that entities fix known software vulnerabilities that could be exploited by a malicious actor through the Internet.

- *CIP-007-6, Requirement R3* requires entities to (1) deploy methods to detect, deter, or prevent malicious code, and (2) mitigate the threat of detected malicious code. This Requirement helps prevent and mitigate the threat of malicious code that may be introduced through Internet connections.

- *CIP-010-2, Requirement R4, Attachment 1* addresses elements included in plans to manage Transient Cyber Assets and Removable Media. Among other things, Attachment 1 requires Responsible Entities to mitigate malicious code on Transient Cyber Assets and Removable Media prior to connecting to medium and high BES Cyber Systems. In addition, Attachment 1 requires Responsible Entities to mitigate the risk of vulnerabilities posed by unpatched software on Transient Cyber Assets. Through these Requirements, the CIP Reliability Standards help to prevent malware propagation to BES Cyber Systems through Transient Cyber Assets and Removable Media.

- *CIP-003-6, Requirement R2, Attachment 1 Section 4 and CIP-008-5, Requirement R1* address Reportable Cyber Security Incidents for low, medium, and high impact BES Cyber Systems. A Reportable Cyber Security Incident is defined as "[a] Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." Responsible Entities must report Reportable Cyber Security Incidents to the E-ISAC, which may include incidents related to malware. The E-ISAC would use its tools to share that information more broadly throughout the industry.

The CIP Reliability Standards promote allocation of resources to the highest risk areas. The currently enforceable CIP Reliability Standards incorporated principles from the National Institute of Standards and Technology Risk Management Framework to categorize and apply security controls.[17] The CIP Reliability Standards include categorization criteria based on the

[17] *See* Background, Reliability Standard CIP-002-5.1, at 3, *available at* http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&jurisdiction=United%20States.

impact of BES Cyber Systems to the reliable operation of the BES.[18] Based on the categorization, the CIP Reliability Standards require Responsible Entities to implement cyber security controls around the BES Cyber Systems that pose the greatest risk to the reliability of the BPS. Responsible Entities can therefore allocate resources appropriately based on the Requirements and risk.

The CIP Reliability Standards also support reliability by balancing cyber security with operational functionality. As outlined in the NOI Comments, "[t]he risk-based framework established in the CIP Reliability Standards seeks to balance the operational needs of responsible entities to have Internet connections to BES Cyber Systems in Control Centers with the security need to protect against Internet borne threats."[19] Data exchange, remote access, patch management, and transmission scheduling capabilities must run smoothly in order for the grid to operate reliably.[20] Therefore, the CIP Reliability Standards are designed to incorporate security practices into these operations without significantly reducing reliability.

The ERO Enterprise's compliance monitoring and enforcement program helps to ensure compliance with the Reliability Standards and continued assessment of the efficacy of the currently enforceable Reliability Standards. Prior to the July 1, 2016 enforceable date, NERC and the Regional Entities conducted extensive outreach to Responsible Entities to assist in the transition to the new version of the CIP Reliability Standards. Since July 1, 2016, the Regional Entities have conducted audits and other compliance monitoring activities assessing Responsible Entities' compliance, and the Commission has collaborated with NERC on additional audits of Responsible Entities. NERC addresses suggested modifications to the CIP Reliability Standards based on

18 *Id.* at 5.
19 *See* NOI Comments at 4.
20 *Id.* at 6-9.

observations during compliance monitoring and enforcement activities through the established standards development process.

B. NERC is developing revisions to its Reliability Standards that will strengthen cyber security, including mitigating risks associated with malware.

Resilient Societies claimed that CIP Reliability Standards do not provide malware protections for communications networks outside the ESP.[21] Further, Resilient Societies commented that the CIP Reliability Standards exempt assets containing low impact BES Cyber Systems from malware protection Requirements.[22] Finally, Resilient Societies asserted that vulnerabilities in cyber supply chains "provide pathways for both malware infection and firmware 'backdoors' into control systems."[23] As discussed below, however, consistent with Commission directives, NERC is currently developing modifications to its CIP Reliability Standards to address these issues, among others.

In response to directives in Order No. 822, NERC initiated a standards development project that addresses further malware protections for assets containing low impact BES Cyber Systems and protections for communications links and sensitive data communicated between BES Control Centers. The standards drafting team clarified electronic access controls and Requirements to mitigate introduction of malicious code from transient devices for assets containing low impact BES Cyber Systems in CIP-003-7, which was approved by the NERC Board of Trustees on February 9, 2017. In addition, the standards drafting team developed draft language on logical protections of communications links transmitting sensitive data between Control Centers of all impact levels (high, medium, and low) for industry comment. The protections extend beyond ESPs if the sensitive data traveled outside ESPs. The proposed revisions enhance protections in

---

21 Petition at 12.
22 *Id.*
23 *Id.* at 10.

the CIP Reliability Standards by, among other things, helping to mitigate some the risks of the introduction of malware to BES Cyber Systems.

Additionally, NERC assembled a standards drafting team to address directives in Order No. 829 on mitigating cyber security risks in the supply chain. The draft Reliability Standard, CIP-013-1, requires Responsible Entities to develop and periodically review a supply chain risk management plan that addresses four security objectives: 1) software integrity and authenticity; 2) vendor remote access; 3) information system planning; and 4) vendor risk management and procurement controls.[24] Furthermore, the draft Reliability Standard requires Responsible Entities to implement at least one process for verifying the integrity and authenticity of certain software and firmware and at least one process to control vendor remote access to high and medium impact BES Cyber Systems. For assets containing low impact BES Cyber Systems, the draft Reliability Standards states that Responsible Entities shall have and periodically review at least one cyber security policy that addresses integrity and authenticity of software and hardware and controls on vendor-initiated remote access. NERC must file this Reliability Standard with the Commission by September 2017. With the development of the draft Reliability Standard, NERC and industry are taking significant steps in addressing the risks posed by malware campaigns targeting supply chain vendors.

Through the NOI, the Commission is also specifically considering additional modifications aimed at mitigating the risks associated with the introduction of malware that could be introduced to BES Cyber Systems at Control Centers. Specifically, the Commission is evaluating the need to isolate BES Cyber Systems in Control Centers from the Internet and the potential need to use

[24] Draft Reliability Standard CIP-013-1, Draft 1, *available at* http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/2016-03_CIP-013-1_draft_Jan_12_2017.pdf.

application whitelisting. As NERC discussed in its comments on the NOI, these controls could help protect BES Cyber Systems from threats such as malware. As NERC also pointed out in its comments, NERC and the Commission need to consider the operational impact of mandating such controls. Given the pending evaluation of these controls and the existing standard development work, it would be premature for the Commission to direct NERC to develop a malware standard, as requested by Resilient Societies.

Aside from the current standards development activity, NERC continuously assesses the efficacy of its Reliability Standards to help determine whether additional revisions are necessary. NERC considers information gathered from compliance monitoring and enforcement activities, known actual or potential threats to the BPS, and other input relevant to the Reliability Standards. At this time, NERC has determined that additional revisions to the CIP Reliability Standards, beyond those under consideration, are not necessary. Nevertheless, NERC will continue to assess the efficacy of the CIP Reliability Standards to help ensure the Reliability Standards include the appropriate protections.

C. NERC engages in other activities related to cyber security that help to reduce risks associated with malware.

NERC's approach to cyber security encompasses more than mandatory Reliability Standards. NERC use a number of security tools outside of the compliance context that have proved to be effective in enhancing the security of the BPS. For instance, through the E-ISAC, NERC has fostered an information sharing culture that promotes a proactive approach towards identification of malware, pooling of resources to combat malware, and sharing of best practices based on lessons learned, among other things.

"The E-ISAC, in collaboration with the DOE and the Electricity Subsector Coordinating Council, serves as the primary security communications channel for the Electricity Subsector and

enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents."[25] Members of the E-ISAC include vetted owners and operators of the BPS. Members receive private-level situational awareness on security threats, physical and cyber security bulletins, access to malware reverse engineering services, remediation, and other security resources. In addition, E-ISAC conducts outreach events to keep industry informed and prepared for cyber security threats. A key service offered by E-ISAC is malware identification and sharing this information with its members.

E-ISAC also leads security exercises every two years, known as GridEx, which simulate widespread, coordinated cyber and physical attacks on critical electric infrastructure. The last such exercise, GridEx III in November 2015, consisted of a two-day simulated security incident and an executive tabletop session featuring 32 industry executives and senior officials from federal and state governments.[26] More than 4,400 individuals from 364 organizations across North America participated in GridEx III, making it the largest geographically distributed grid security exercise to date.[27] GridEx IV is planned for November 2017. These events help strengthen entities' crisis response functions, which can be used to handle attacks from malware, and provide input for lessons learned.

Aside from E-ISAC activities, NERC also provides information sharing and learning opportunities that enhance industry practices in cyber security. NERC hosts the annual Grid Security Conference ("GridSecCon"). At GridSecCon, cyber security and physical security

---

25 *See* E-ISAC Vision, *available at* https://www.esisac.com/#about.

26 *The Electricity Sector's Efforts to Respond to Cybersecurity Threats: Hearing before the Subcomm. On Energy of the H. Comm. On Energy and Commerce*, 115th Cong. 9-10 (2017) (statement of Gerry W. Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation), *available at* http://docs.house.gov/meetings/IF/IF03/20170201/105497/HHRG-115-IF03-Wstate-CauleyG-20170201.pdf.

27 *Id.* at 9.

experts from industry and government convene to share emerging security trends, policy advancements, and lessons learned related to the electricity sector.[28]

In addition, NERC communicates and works with industry to facilitate necessary information sharing. First, NERC issues NERC Alerts to provide security information to the electricity industry.[29] NERC Alerts can range from purely informational bulletins to identification of actions deemed essential to BPS reliability.[30] In 2016, NERC issued an alert related to the cyber security event in Ukraine. The alert focused on mitigating adversarial manipulation of industrial control systems based on lessons learned from the event. Second, 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. For instance, in November 2015, a CIPC subcommittee developed guidelines for the electricity sector on control system electronic connectivity.[31] The guidelines identify industry recommendations on securing control system networks from threats, such as malware. Development of guidelines is an ongoing activity for CIPC that occurs in response to actual or potential threats or risks.

Finally, NERC and the Regional Entities provide continual outreach to industry to share best security practices. In November 2016, NERC hosted the Emerging Technology Roundtable on Substation Automation and International Electrotechnical Commission ("IEC") 61850 and

---

28 *Id.* at 11.

29 NERC Alerts, *available at* http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx.

30 *The Electricity Sector's Efforts to Respond to Cybersecurity Threats: Hearing before the Subcomm. On Energy of the H. Comm. On Energy and Commerce*, 115th Cong. 8 (2017) (statement of Gerry W. Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation), *available at* http://docs.house.gov/meetings/IF/IF03/20170201/105497/HHRG-115-IF03-Wstate-CauleyG-20170201.pdf.

31 *Security Guidelines for the Electricity Sector: Control System Electronic Connectivity*, Critical Infrastructure Committee, Control Systems Security Working Group, Sep. 25, 2016, *available at* http://www.nerc.com/comm/CIPC/Control%20Systems%20Security%20Working%20Group%20CSSWG%202013/Control%20Systems%20Electronic%20Connectivity%20guideline.pdf.

Cloud Computing, which included discussion of the threat of malware to Control Centers.[32] Regional Entities also give workshops for entities within their regional footprints covering security topics. In addition, NERC and the Regional Entities hold webinars to increase industry awareness on security practices.

Through these activities, NERC promotes the necessary information sharing of cyber security threats and helps foster the type of incident reporting sought in the Petition.

[32] *Session Recordings: Emerging Technology Roundtable – Substation Automation/IEC 61850* (Nov. 15, 2016), *available at* http://www.nerc.com/pa/CI/Documents/roundtable%20recording%20details%20-%20IEC%2061850%20%20(20161115).pdf; *Session Recordings: Emerging Technology Roundtable – Cloud Computing* (Nov. 16, 2016), *available at* http://www.nerc.com/pa/CI/Documents/roundtable%20recording%20details%20-%20cloud%20computing%20%20(20161116).pdf.

II. CONCLUSION

For the reasons stated above, NERC respectfully requests the Commission deny the Petition for rulemaking submitted by Resilient Societies. The currently enforceable CIP Reliability Standards include protections for BES Cyber Systems from the introduction of malware. In addition, NERC's current standards development activity is focusing on enhancements to the existing CIP Reliability Standards that will address, among other things, risks associated with malware. Finally, NERC and the E-ISAC work to facilitate information sharing among entities to identify and mitigate attacks from malicious actors and other threats to the security of the BPS. Nonetheless, NERC and the Commission will continue to review the CIP Reliability Standards for opportunities to increase their efficacy in protecting the BPS from the risk of malware and will consider modifications when appropriate. Therefore, the Commission does not need to direct further revisions to the CIP Reliability Standards at this time.

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
(202) 644-8099 – facsimile
shamai.elstein@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 17, 2017

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 No. AD17-9-000.

Dated at Washington, DC this 17th day of February, 2017.

/s/ Courtney M. Baughan

Courtney M. Baughan
Legal Assistant
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
courtney.baughan@nerc.net