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