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
mailto: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