PUBLIC VERSION
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED PURSUANT TO 18 C.F.R. § 388.112

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RR19-7-001**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE ORDER ON THE FIVE-YEAR PERFORMANCE ASSESSMENT

Nina Jenkins-Johnston
Senior Counsel
Shamai Elstein
Assistant General Counsel
Candice Castaneda
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000

nina.johnston@nerc.net
shamai.elstein@nerc.net
candice.castaneda@nerc.net

Counsel for the North American Electric Reliability Corporation

June 1, 2020

PUBLIC VERSION
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED PURSUANT TO 18 C.F.R. § 388.112

TABLE OF CONTENTS

PUBLIC VERSION
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED PURSUANT TO 18 C.F.R. § 388.112

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RR19-7-001**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO THE ORDER ON THE FIVE-YEAR PERFORMANCE ASSESSMENT

The North American Electric Reliability Corporation ("NERC") hereby submits this compliance filing in accordance with the Federal Energy Regulatory Commission's ("Commission") January 23, 2020 Order on the Five-Year Performance Assessment ("Order").[1] In that decision, the Commission directed NERC to submit a compliance filing within 90 days of the Order on the following areas:[2]

(i) Oversight of Regional Entities;

(ii) Development of Reliability Guidelines; and

(iii) Clarifications regarding the Electricity Information Sharing and Analysis Center ("E-ISAC").

Regarding the first area, Oversight of Regional Activities, this compliance filing provides an overview of NERC's ongoing program area oversight of Regional Entity activities as part of

[1] *Order on Five Year Performance Assessment*, 170 FERC ¶ 61,029 (2020) [hereinafter Order].

[2] The Order also directed a second compliance filing regarding enhancements to the NERC Rules of Procedure ("ROP"). That compliance filing is on schedule for timely submission to the Commission. *See also, N. Am. Elec. Reliability Corp.*, "Notice of Extension of Time," Docket No. RR19-7-000 (Feb. 28, 2020) (delegated letter order) (granting an extension through August 28, 2020 for the second compliance filing as further extended in the same docket through September 28, 2020).

NERC's regular business functions, NERC's current, targeted approach to Regional Entity audits conducted by the NERC Internal Audit function, and how NERC proposes to enhance its audits of Regional Entities going forward.[3]

To address the second area, Development of Reliability Guidelines, this compliance filing explains how it determines whether a Reliability Guideline is an appropriate method to address a potential risk to reliability, how NERC develops Reliability Guidelines, and how NERC evaluates Reliability Guideline effectiveness. NERC is enhancing its evaluation process under the framework and metrics detailed below. NERC will use this enhanced methodology to examine whether NERC should incorporate components of a particular Reliability Guideline into Reliability Standards at least once every three years.

Finally, NERC provides more information regarding the feedback loop between the E-ISAC and Reliability Standards, the relationship between the E-ISAC and Electricity Subsector Coordinating Council ("ESCC"), and E-ISAC performance metrics. NERC respectfully requests that the Commission accept this submittal in response to the Order.

I. NERC Oversight of Regional Entities

The Commission's Order stated that it, "support[ed] NERC's goal of performing oversight in a risk-based manner."[4] However, the Commission provided, "[w]e continue to believe that performing a comprehensive audit of the Regional Entities' compliance with the CMEP, as outlined in Appendix 4A, once every five years is necessary for NERC to confirm that the Regional Entities are performing their delegated responsibilities adequately."[5] The Commission concluded:

---

[3] *See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104 at PP 321-37, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006) [hereinafter Order No. 672].

[4] Order, *supra*, at P 47.

[5] *Id.* at P 53

> We direct NERC to submit in a compliance filing …: (1) a definitive statement of whether NERC has performed any audits of the Regional Entities during the performance assessment period covering the scope of Appendix 4A, and if so, provide its audit reports in compliance with its Rules of Procedure; and (2) if it has not performed such audits, provide a plan to perform those audits within the next 18 months and going forward. If NERC would like to implement an alternative oversight process for the Regional Entities that it believes is as efficient and effective as the comprehensive audits conducted every five years, then its compliance filing should include a detailed explanation of how its oversight process accomplishes the aims of Order No. 672. The Commission would then determine whether Appendix 4A and the regional delegation agreements should be amended to align with NERC's oversight process.[6]

As documented in the 2019 ERO Performance Assessment, NERC's comprehensive oversight of the Regional Entities includes two sets of coordinated work streams: (a) each NERC business function provides ongoing oversight and program development of activities under its scope of responsibility; and (b) NERC Internal Audit conducts formal audits. This coordination is beneficial in that it ensures that NERC Internal Audit acts as a check on the oversight activities conducted by the NERC business functions while avoiding duplication of efforts. Communication between NERC business functions and NERC Internal Audit provides a feedback loop supporting effective and efficient oversight. This section of the compliance filing outlines the oversight of Regional Entity activities by NERC's business functions and NERC's Internal Audit targeted process for conducting audits of the Regional Entities during the Assessment Period.[7]

In addition to further describing the current oversight structure that is in place, NERC proposes to enhance the NERC Internal Audit-led portion of the process through an expansion of the scope of certain audits already taking place on a regular basis. These audits, led by NERC

---

6 *Id.* at P 54 (internal citations omitted).

7 The Assessment Period covered June 1, 2014 – December 31, 2018.

Internal Audit with the assistance of external observers, currently focus on CMEP and Organization Registration and Certification Program ("ORCP") activities of NERC. As proposed, they would encompass CMEP and ORCP activities of the entire ERO Enterprise. They would replace the audits contemplated in Attachment 4A of the NERC Rules of Procedure ("ROP")[8] and would address the principles outlined by the Commission in Order No. 672.[9]

A. NERC Business Function Oversight Activities

As noted above, NERC performs ongoing oversight of the Regional Entities through its business functions using monitoring tools identified in their oversight plans. The CMEP and ORCP business functions document their oversight in the following public reports:

(i) Quarterly reports to the NERC Board of Trustees ("Board") describing key metrics and trends for processing of noncompliance;[10]

(ii) An annual CMEP Report, which consolidates metrics for the year, details lessons learned, and identifies forward-looking activities regarding implementation of the regulatory programs by the Regional Entities;[11] and

(iii) Process reviews to evaluate alignment (i.e., reviews of registration requests, certifications, mitigation plans, self-logging, settlements and penalties, audit report, compliance exceptions and FFTs after posting sampling).[12]

The Reliability Assessment, Performance Analysis, Event Analysis, and Bulk Power System Awareness business functions focus their oversight on:

---

[8] A high-level description of potential changes to the ROP is included for illustration only. A formal process for developing revised rules would be initiated upon Commission approval of this proposal.

[9] *See*, *supra*, Order No. 672.

[10] *See*, *e.g.*, Compliance Monitoring and Enforcement Program Quarterly Report Q3, 2019 (Nov. 1, 2019), available at https://www.nerc.com/pa/comp/CE/ReportsDL/Q3%202019%20Quarterly%20CMEP%20Report.pdf.

[11] *See*, *e.g.*, Compliance Monitoring and Enforcement Program Annual Report (Feb. 5, 2020), *available at*, https://www.nerc.com/pa/comp/CE/ReportsDL/2019%20Annual%20CMEP%20Report.pdf.

[12] *See*, *e.g.*, NERC Review for the Annual FFT CE Sampling Program, Docket No. RC11-6-009 (filed Aug. 16, 2019), available at https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Public%20FFT%20Sampling%202019%20-%20closure_final.pdf.

(i) Promoting high standards of quality, consistency, and timeliness in reporting of data required to produce the various reliability assessments for the ERO (i.e., long-term, summer, winter, and probabilistic);

(ii) Evaluating the progress and status of events within the Event Analysis Process;

(iii) Evaluating progress on lessons learned development; and

(iv) Ensuring reporting is complete and validated in data collection applications, such as GADS, TADS, and MIDAS.[13]

Ongoing evaluation of program activities by these business functions supports consistent effective and efficient performance of delegated activities concerning CMEP, ORCP, and Reliability Assessment activities.

B. NERC Audits of the Regional Entities during the Assessment Period

As noted above, NERC Internal Audit conducts formal audits as part of NERC's overall oversight of the Regional Entities. These audits are risk-based, and audit topics are identified through a variety of inputs. First, NERC Internal Audit identifies and prioritizes inherent and residual risks in the ERO's operations as part of its regular enterprise risk management activities.[14] NERC Internal Audit also works with each business function to understand oversight activities for the various Regional Entity delegated activities, consistent with their business oversight plans. Finally, NERC Internal Audit maps business oversight activities against requirements (referred to as "shall statements") in the ROP and Regional Delegation Agreements ("RDAs"). This mapping allows Internal Audit to evaluate NERC business oversight of Regional Entity obligations and determine whether specific areas require further examination directly by Internal Audit. For the aforementioned audits, Internal Audit looked at the processes underlying the applicable "shall

[13] GADS is Generating Availability Data System, TADS is Transmission Availability Data System, and MIDAS is protection system Misoperations Information Data Analysis System.

[14] Inherent risk represents a risk to NERC without considering the internal controls NERC has in place to mitigate the risk. Residual risk is what remains after the implementation of internal controls.

statements" and potential process improvements. Final audit reports reflect any findings of noncompliance as well as observations and recommendations related to process improvements.

In its Order, the Commission directed NERC to submit a definitive statement whether NERC audited the Regional Entities and provide any audit reports in compliance with the ROP.[15] During the Assessment Period, NERC conducted two Compliance Monitoring and Enforcement ("CMEP") Audits of the Regional Entities, pursuant to Section 401.1.3 of the NERC ROP (*see* **Attachment 2**).[16] These audits examined: (i) Confidential Information and conflict of interest procedures, and (ii) internal controls evaluations of registered entities as part of compliance monitoring. In addition to the two CMEP Audits, during the Assessment Period, NERC conducted two non-CMEP Audits of the Regional Entities examining: (i) implementation of the event analysis process, and (ii) Section 215 accounting by Regional Entities that perform non-Section 215 statutory activities. The relevant audit reports are attached (**Attachment 2**). NERC requests that the Commission treat these audit reports as privileged material in accordance with 18 C.F.R. §388.112. The Commission should treat this material as confidential and non-public because it reflects confidential business information as well as NERC's investigative audit process. NERC has attached a proposed model form of protective agreement as **Attachment 1**.

C. Proposed Enhancements to Regional Entity Oversight

In its Order, the Commission states that if NERC wishes to "implement an alternative oversight process for the Regional Entities that it believes is as efficient and effective as the

---

15 Order, *supra*, at P 54.

16 NERC requests that the Commission treat the Appendix 4A and Section 1207 Regional Entity audit reports, included with this compliance filing as Attachment 2, as privileged material in accordance with 18 C.F.R. §388.112. The Commission should treat this material as confidential and non-public, because it reflects confidential business information as well as NERC's investigative audit process. NERC has attached a proposed form of protective agreement as Attachment 1.

comprehensive audits conducted every five years, then its compliance filing should include a detailed explanation of how its oversight process accomplishes the aims of Order No. 672."[17]

NERC proposes to enhance the process for Regional Entity audits completed by Internal Audit, which, as indicated, is one piece of NERC's overall oversight of the Regional Entities. No changes are being proposed to how NERC business functions conduct oversight activities; the comprehensive process for Regional Entity Oversight is documented in the 2019 ERO Performance Assessment in this docket.

In this section, NERC describes its alternative approach to formal audits of Regional Entities and how that approach is consistent with the following requirements in Order No. 672:

(i) Audits within a defined frequency;

(ii) Commission visibility into results (i.e., submission of audit reports); and

(iii) Commission participation in any audit of Regional Entities.

Specifically, NERC proposes to enhance its process when auditing Regulatory Programs to include them within NERC's three-year Independent Audit and to continue Non-Regulatory Audits pursuant to Section 1207 of the ROP as follows:

(i) Regulatory Programs Audit: conducted at least once every three years (possibly through an independent auditor) with CCC and Commission observers, which examines all "shall statements" associated with the CMEP, ORCP, and BES Exception functions (collectively, Regulatory Programs); and

(ii) Non-Regulatory Programs Audit: conducted annually with Commission observers, which examines all "shall statements" associated with other delegated functions performed by the Regional Entities outside of the Regulatory Programs.

[17] Order, *supra*, at P 54.

To accomplish these proposed enhancements, NERC would initiate the process for amending the ROP (and any necessary conforming changes for NERC Regional Delegation Agreements) as follows:

(i) Expand the scope of the audits of NERC contemplated in Sections 406 and 506 of the ROP to encompass ERO Enterprise CMEP and ORCP activities.

(ii) Clarify that Sections 406 and 506 of the ROP allow CCC and Representatives from Applicable Governmental Authorities to participate as observers in such audits.

(iii) Make conforming changes to eliminate references to Appendix 4A and remove Appendix 4A in its entirety, in light of the proposed consolidation of separate Regional Entity audit procedures with Sections 406 and 506 of the ROP.

1. Regulatory Programs Audit

NERC Internal Audit will conduct the Regulatory Programs Audit and may leverage the assistance of an independent auditor to conduct this audit at least once every three years. Consistent with the ERO Enterprise model, this audit of NERC will examine "shall statements" for which NERC and the Regional Entities are individually and collectively responsible. Internal Audit will conduct these audits at NERC's Atlanta and/or Washington, D.C. offices. In response to audit queries and requests for evidence from Internal Audit, NERC will collect relevant evidence from its business functions as well as from the Regional Entities to demonstrate both NERC and Regional Entity adherence to the ROP. NERC Internal Audit will determine the specific scope of each audit in collaboration with any independent auditors and participating observers. NERC Internal Audit also will document any risk assessment methods used in connection with the scoping process.

Commission and CCC representatives may participate as observers, at their respective discretion. Public posting of audit reports will occur upon mitigation of all findings in the final audit report. NERC will submit this audit report to the Commission following submission to the

NERC Board. Since this audit will occur once every three years, Internal Audit will continue to conduct self-certifications (for both NERC and the Regional Entities) for a subset of applicable "shall statements" in any year in which this audit does not occur.

2. Non-Regulatory Programs Audit

NERC proposes to continue conducting a second type of audit consistent with Section 1207 of the ROP of the Regional Entities examining topics outside of the Regulatory Programs. Like the Regulatory Programs Audit, this audit will examine "shall statements" in the NERC ROP as they apply to the Regional Entities. Similar to the Regulatory Programs Audit, NERC Internal Audit will perform this audit.[18] NERC Internal Audit will identify the scope using its risk assessment process for a given year (i.e., heat maps and determination of residual risk).[19] Commission representatives may participate as observers consistent with Order 672. Non-regulatory topics could include, for example, the event analysis program and accounting for statutory versus non-statutory regional activities. NERC will submit this audit report to the Commission following submission to the NERC Board.

Including Regulatory Program Audits within NERC's independent audit of CMEP and ORCP activities will support a robust, independent, audit that is consistent with the intent in Order No. 672, while enhancing frequency of audits, increasing efficiency, and streamlining procedures. Further, the approach for Non-Regulatory Audits will ensure that NERC conducts risk-based monitoring for Regional Entity compliance with ROP obligations beyond those associated with Regulatory Programs. As a result, NERC's proposal is more effective and efficient than a single 5-year audit.

---

[18] NERC may rely on an independent auditor as NERC determines appropriate.

[19] More than one topic can be selected and more than one audit performed.

II. NERC Guidance Development Process

The Order also requested additional detail regarding NERC Reliability Guidelines,[20] and directed that NERC explain:

> (1) its guidance development process; including how and when it evaluates the need to develop, approve, and post a guideline document; (2) the methodology and metrics NERC proposes to use to determine if that guidance document is addressing the risks that led to its development; and (3) how and at what interval NERC will evaluate whether components of the guidance document should be incorporated into the Reliability Standards.[21]

This compliance filing answers each question posed by the Commission.

As recognized in the Order,[22] Reliability Guidelines are one of the ERO Enterprise's tools for a risk-based approach to reliability. NERC's reliability, resilience, and security toolkit includes, but is not limited to: industry outreach events, Reliability Guidelines, Alerts, Reliability Standards, ORCP, and CMEP. In addition, the ERO Enterprise engages forums and industry trade associations to assist with developing best practices, awareness, Implementation Guidance,[23] Reference Documents, and other solutions to address identified risks. NERC carefully evaluates whether a Reliability Guideline is the best approach to managing a potential risk to reliability. NERC has worked with its ERO Enterprise partners and presented the framework detailed below to formalize evaluation of whether a Reliability Guideline is the best solution to address an issue and its effectiveness. Throughout the Assessment Period, the ERO Enterprise continued to lead industry in reliability, resilience, and security initiatives, such as Reliability Guidelines, to identify risks and engage industry in a collaborative approach to mitigating those risks.

---

[20] Order, *supra*, at PP 56-59.
[21] *Id.* at P 59.
[22] *Id.* at PP 56-58.
[23] NERC's Compliance Guidance Policy is available at https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy%20-%20BOT%20Approved%2011_05_2015a.pdf.

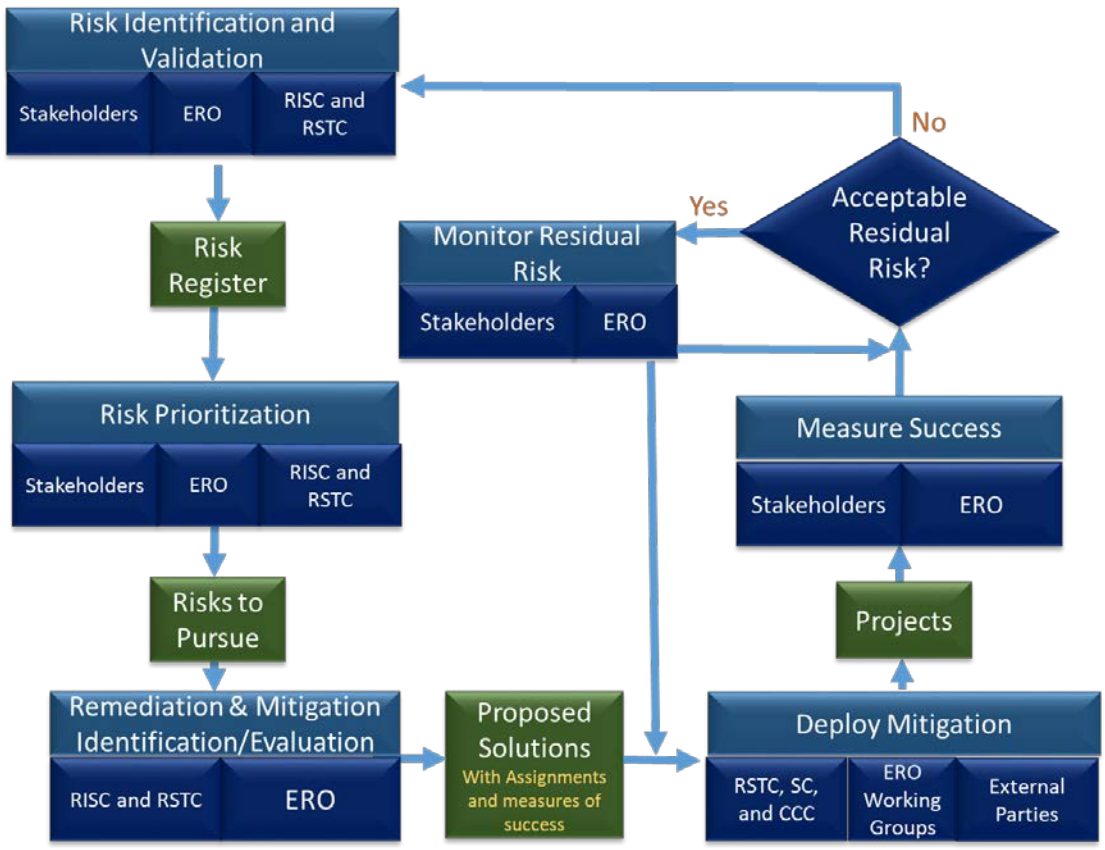
Reliability Guidelines serve a unique function by outlining approaches for managing potential risks to reliability in a particular area. They are distinct from, and not intended to replace, mandatory and enforceable Reliability Standards. Reliability Standards set forth requirements for Reliable Operation of the Bulk-Power System ("BPS"). NERC Reliability Standards specify clear reliability objectives so that responsible entities can make optimal planning, operating, and resource determinations that meet stated performance requirements. Reliability Guidelines, on the other hand, provide detailed approaches and methods to address a reliability concern based on technically sound experience of subject matter experts and diverse stakeholders.

A Reliability Guideline often addresses a new or rapidly evolving reliability risk (e.g., Reliability Guideline: *BPS-Connected Inverter-Based Resource Performance*). At times, a Reliability Guideline, such as the Guideline on Gas and Electrical Operational Coordination, may provide guidance on an area not directly addressed by a Reliability Standard. In other instances, a Reliability Guideline may exist in harmony with a Reliability Standard touching upon the same area. For example, Reliability Standards VAR-001-4.1, VAR-002-4, and TPL-001-5 provide reactive power requirements for planning and operations. The Reactive Power Planning Guideline provides industry guidance on how to achieve those obligations while considering the needs associated with local reliability. NERC carefully considers whether Reliability Guidelines, enforceable Reliability Standards, Alerts, or other measures are the best way to approach a potential reliability challenge, in light of the circumstances.

NERC is now working with the Reliability Issues Steering Committee ("RISC") to formalize a six-step framework to address known and emerging reliability and security risks.[24]

[24] *Reliability Issues Steering Committee Agenda*, April 1, 2020 (Item 2), https://www.nerc.com/comm/RISC/Agenda%20Highlights%20and%20Minutes/RISC_Agenda_Package_April%201_2020.pdf.

During the Assessment Period, NERC informally evaluated these questions. The framework below outlines the process. Consistent with risk management frameworks used by other organizations and industries, these six steps include: 1) Risk Identification; 2) Risk Prioritization; 3) Mitigation Identification and Evaluation; 4) Deployment; 5) Measurement of Success; and 6) Monitoring. The following section details how NERC would implement these steps: a) to determine whether a Reliability Guideline is the appropriate approach to mitigate a potential risk (Steps 1-3); b) the Reliability Guideline development process (Step 4); and c) NERC's proposed enhanced methodology for evaluating the effectiveness of Reliability Guidelines (Steps 5-6). The figure below provides a flow chart of the process outlined above, and the following discussion will explain how Reliability Guidelines fit within that framework.



A. Determining Whether a Reliability Guideline is Appropriate

As noted above, NERC applies 1) Risk Identification; 2) Risk Prioritization; and 3) Mitigation Identification and Evaluation to determine whether a Reliability Guideline is an appropriate solution to help mitigate potential risks to reliability.

1. Risk Identification

NERC works continuously with industry subject matter experts to identify and validate risks to reliable and secure operation of the BPS based on analysis of system performance. In addition, the RISC brings together industry experts to identify and prioritize emerging risks, as well as suggest mitigation activities. ERO Enterprise leadership and the RISC partner to capture input from ERO program areas, industry forums, and trade associations on existing and emerging risks. NERC might identify risks, for example, through:

1. ERO Enterprise stakeholder-supported technical organizations, Compliance Forums, and associated subject matter experts
2. Focused compliance monitoring activities
3. Reliability Assessments
4. Events Analysis
5. Analysis of Availability Data Systems (TADS, GADS, DADS, MIDAS, etc.)
6. Frequency Response, Inertia, and other essential reliability service measurements
7. Interconnection simulation base case quality and fidelity metrics
8. RISC Biennial Risk Report
9. Regional Risk Assessments
10. External parties (Department of Energy, Department of Homeland Security, Natural Resources Canada, EPRI, etc.)
11. Shared public and/or government intelligence and emphasis (e.g., continued emphasis on cybersecurity among all industries, focus on journalism, and expressed public policy focus by all branches of government)

2. Risk Prioritization

After identifying a risk, NERC works with its committees to validate the magnitude and priority of the risk. NERC prioritizes risks through analysis of potential exposure, scope, and duration, as well as impact and likelihood. NERC collects data to support this analysis during Risk

Identification. NERC applies technical expertise to decide whether identified risks require near-term mitigation or continued monitoring. Depending on the complexity of the situation, NERC may need to develop new models, algorithms, and processes to examine the risk. This process would be consistent with other risk management frameworks, and NERC tested the process through a RISC-issued survey based on the risks that group prioritized in early 2019.

3. Mitigation Identification and Evaluation

Finally, NERC identifies and evaluates the best mitigation activity to address a particular risk, balancing effective and efficient use of resources and the potential risk impact and likelihood. To complete this analysis, NERC examines the following factors, with input from stakeholder subject matter experts:[25]

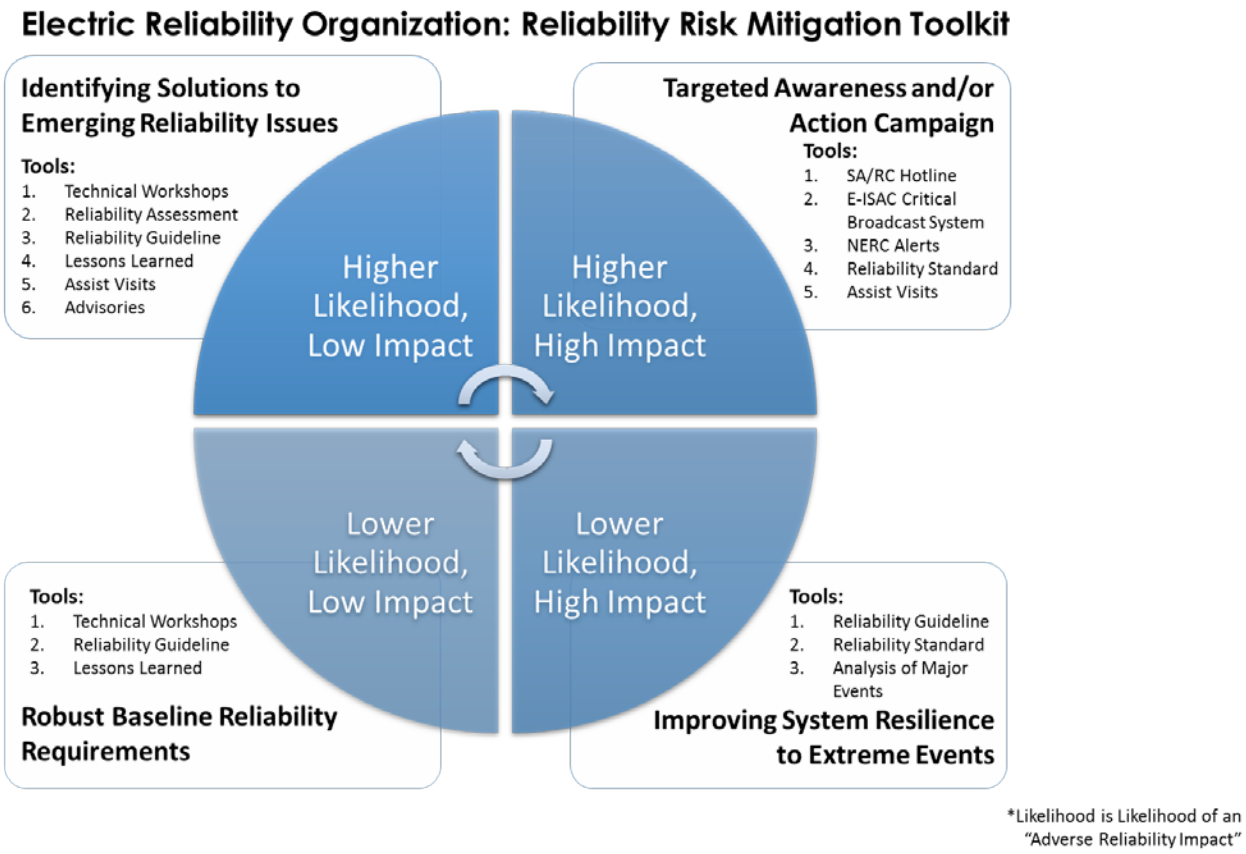
1. What is the potential impact or severity of the risk?
2. How probable is the risk? Is it sustained, decreasing, or growing?
3. Is the risk here today or anticipated in the next 3-5 years?
4. How pervasive is the risk?
5. Is mitigation expected to be a one-time action, or ongoing?
6. Have we had experience with events being exacerbated by the risks, or there is no experience, but the probability is growing (i.e. cyber or physical)?
7. Have previous mitigation efforts been deployed? If so, were they effective? Why or why not?
8. What is an acceptable residual risk level after mitigating activities have been deployed?
9. Is the risk human-made or by natural/human-error causes?

Once NERC prioritizes risks, NERC and stakeholder subject matter experts recommend potential mitigation measures and assess their expected effectiveness. As noted above, mitigation activities could include Reliability Standards, Reliability Guidelines, Technical Engagement, Reliability Assessment, and Alerts, as well as other mechanisms in NERC's reliability toolkit.

[25] Subject matter expertise might be provided, for example, by the ERO Enterprise and its stakeholders (such as standing technical committees and their subgroups, or standard drafting teams), and external parties, such as the North American Transmission and Generation Forums (NATF and NAGF), North American Energy Standards Board (NAESB), the Institute of Electrical and Electronic Engineers (IEEE), and EPRI.

Reliability Guidelines are particularly useful for addressing: i) moderate impact sustained risks that are unlikely; and (ii) low impact sustained risks that are unlikely or likely. NERC also uses Reliability Guidelines to address risks in areas that may in some portion fall outside NERC's jurisdiction (e.g., Reliability Guideline: *BPS Reliability Perspectives on the Adoption of IEEE 1547-2018*). Reliability Guidelines enable the ERO Enterprise to highlight expectations or priorities on appropriate practices for a given subject area. The Reliability Guideline development process detailed below provides flexibility and responsiveness while maintaining technical rigor. Together with the baseline fabric provided by Reliability Standards, Reliability Guidelines are an important tool in the suite of ERO mechanisms for addressing risk. Reliability Guidelines may also establish performance expectations for emerging risks prior to codifying such expectations into Reliability Standards.

The following figure illustrates where Reliability Guidelines fit within Mitigation Identification and Evaluation:



B. Reliability Guideline Development Process for Deployment

Technical committee charters set forth NERC's Reliability Guideline development process for deployment of a guideline in response to a risk. During the Assessment Period, Reliability Guideline development fell within the Operating Committee, Planning Committee, and Critical Infrastructure Protection Committee Charters. Going forward, the Reliability and Security Technical Committee ("RSTC") Charter consolidates these procedures.[26] This consolidation will

[26] RSTC Charter, Section 8 (effective Nov. 5, 2019), available at, https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf.

The RSTC is a standing committee that strives to advance the reliability and security of the interconnected Bulk-Power System of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission.
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board, and ERO Enterprise staff and leadership.
- Coordinating and overseeing implementation of RSTC subgroup work plans.

ensure that one central committee develops and evaluates all Reliability Guidelines on a uniform basis. Developing Reliability Guidelines through technical committee proceedings also ensures transparency. RSTC work plans will reflect proposals for Reliability Guidelines, and the RSTC Charter requires an open and transparent notice and comment process.

Under the RSTC Charter, the Committee or one of its subgroups determines whether to develop a Reliability Guideline. A variety of drivers might give rise to this step, including, for example, Reliability Assessments, RISC reports, NERC Staff input, or Reliability Standard implementation. When the RSTC or a subgroup observes a potential risk to reliability, the RSTC evaluates mitigation measures per the first three steps of the framework described above. A Reliability Guideline is one approach to address such a risk. For example, the NERC Operating Committee and Planning Committee approved the Reliability Guideline: Methods for Establishing IROLS[27] after the Method for Establishing IROLs Task Force surveyed Reliability Coordinators on whether reliability considerations might arise from the use of different methods.

The diversity of factors that may give rise to Reliability Guidelines reflects their responsive nature within NERC's toolkit for reliability. The RSTC or its subgroups then develop the Reliability Guideline. The Committee must then approve posting any Reliability Guideline for 45-day public comment. After the comment period closes, the RSTC must publish comments and responses. Next, a new or updated Guideline is presented to the RSTC for approval. After RSTC approval, NERC posts Guidelines on NERC's website.

[27] NERC, *Reliability Guideline: Methods for Establishing IROLs* (Sept. 2018), available at https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf. *See also*, IROL Framework.

C. Measuring Success and Monitoring Effectiveness of Reliability Guidelines

The RSTC continues to evaluate Reliability Guidelines after approval and posting, consistent with Measurement of Success and Monitoring in the Framework introduced above. This review process ensures timely evaluation of Reliability Guidelines, while not precluding the development of any new or revised Reliability Standards addressing the same topic, particularly if NERC or a stakeholder submits a Standard Authorization Request identifying an urgent need.

The Committee accepts comments on Reliability Guidelines on an ongoing basis and must review comments on a quarterly basis. At any time, the RSTC may decide to update a Reliability Guideline based on such comments or changes in industry. Further, at a minimum of every third year from a Guideline's last revision, the RSTC must review the Reliability Guideline for continued applicability, usefulness, and effectiveness.

NERC intends to apply the following methodology to evaluate whether a Reliability Guideline is addressing the risks that led to its development. The RSTC work plan will reflect Committee activities to evaluate Reliability Guidelines. Under NERC's proposed methodology, the RSTC would assess industry's implementation and effectiveness of: i) existing Reliability Guidelines two years after the RSTC's initial full meeting on June 10-11, 2020, and ii) two years after the RSTC approves a new or revised Reliability Guideline.

The RSTC will rely on these surveys and other available information to review Reliability Guidelines triennially using the following metrics:[28]

[28] The RSTC would evaluate pre-existing Guidelines three years after the RSTC's initial full meeting June 10-11, 2020.

Metrics for Evaluation of Reliability Guidelines:

- Performance of the BPS prior to and after a Reliability Guideline, as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments);
- Use and effectiveness of a Reliability Guideline as reported by industry via survey;
- Industry assessment of the extent to which a Reliability Guideline is addressing risk as reported via survey; and
- Development of metrics specific to each Reliability Guideline, included within a Reliability Guideline by the RSTC (or a committee subgroup): a) during triennial review of existing Reliability Guidelines; and b) during creation/revision of Reliability Guidelines.[29]

Once this evaluation is complete, the RSTC would present a recommendation to NERC on: a) the effectiveness of a Reliability Guideline, and b) whether risks warrant additional mitigation measures (i.e., Reliability Standards, Alerts, industry outreach, etc.).

In addition to RSTC review, the NERC State of Reliability and Reliability Assessment reports provide feedback on the effectiveness of Reliability Guidelines. In developing these reports, NERC and the Regional Entities gather quantitative and qualitative data on reliability trends and emerging issues. For example, the 2019 State of Reliability report highlighted industry's implementation of the Inverter-Based Resource Performance Guideline as a measure helping to manage the increasing integration of these resources on the BPS.

After receipt of the RSTC's recommendation, NERC would evaluate the RSTC's review, analysis by NERC Reliability Assessments, and any other relevant data in NERC's possession to determine whether additional action might be appropriate to address potential risks to reliability.

[29] The RSTC will expect that Reliability Guidelines in development include metrics on their effectiveness.

III. Electricity Information Sharing and Analysis Center

The Commission also directed that NERC supply additional information regarding the E-ISAC within 90 days of the Order and update the E-ISAC-related provisions in the ROP within 180 days of the Order (as extended through September 28, 2020).[30] The Order provided that this first compliance filing should include information on: 1) the feedback loop between the E-ISAC and Reliability Standards;[31] 2) NERC's relationship with the Electricity Subsector Coordinating Council's ("ESCC") Member Executive Committee ("MEC");[32] and 3) the E-ISAC's performance metrics.[33] The following supplement to the record addresses each area highlighted in the Order.

A. E-ISAC and Reliability Standards Coordination

The Order directed that NERC provide details regarding:

> (1) [H]ow NERC receives information from the E-ISAC and how the EISAC determines what data to share with NERC; and (2) once NERC receives such information, what NERC does with the information and how NERC determines whether such information is used to develop or inform the development of Reliability Standards. We emphasize that we are not seeking to obtain any specific information in the compliance filing that industry may submit to the E-ISAC. Instead, we seek, generally, a better understanding of how the E-ISAC informs the development of Reliability Standards.[34]

NERC appreciates this opportunity to clarify E-ISAC information sharing practices and the manner in which the E-ISAC may help inform the development of Reliability Standards.

As discussed in NERC's Performance Assessment, E-ISAC information exchange with the Standards Department must comply with the E-ISAC Code of Conduct's restriction on sharing

---

30 *See*, *supra*, note 2. NERC is updating E-ISAC-related provisions of the ROP, and NERC is on schedule to submit a timely compliance filing presenting those revisions to the Commission.
31 Order, *supra*, at P 68.
32 *Id.* at P 70
33 *Id.* at P 72.
34 *Id.* at P 68.

voluntarily-provided information across the ERO. The E-ISAC Code of Conduct governs the information sharing relationship between the E-ISAC and other NERC departments and outlines the parameters within which E-ISAC personnel may share member-provided information outside the E-ISAC.[35]

While a primary focus of the Code of Conduct is to ensure that information members share with the E-ISAC is not shared with, reported to, or used by CMEP personnel to enforce NERC Reliability Standards, the information sharing restrictions go beyond a simple restriction on conveying violation information to CMEP personnel. To promote robust information sharing within the electric industry, the E-ISAC Code of Conduct establishes broad information sharing restrictions. It generally restricts E-ISAC personnel from sharing any Protected Information, as that term is defined in the Code of Conduct, with any non-E-ISAC personnel at NERC. The E-ISAC Code of Conduct defines Protected Information broadly to include all non-public information voluntarily reported to the E-ISAC that is not otherwise reported to other NERC departments.[36]

---

[35] The E-ISAC Code of Conduct is available at https://www.eisac.com/Documents/E-ISAC_Code_of_Conduct.pdf (capitalized E-ISAC terms not defined herein have the meaning ascribed in the Code of Conduct).

[36] The E-ISAC Code of Conduct provides that:

> 2.10 Protected Information
>
> A subset of E-ISAC Information that is voluntarily reported to assist the E-ISAC in its analysis and identification of emerging threats and that is not otherwise reported to any other NERC department. Protected Information is generally provided to the E-ISAC as "***Attributed Protected Information***", which is Protected Information that contains the identity of the entity reporting the information and/or the identities of other entities and/or information about specific locations of assets that may be subject to threats or vulnerabilities as set forth in the Protected Information submitted to the E-ISAC. "***Unattributed Protected Information***" is Protected Information that that does not contain the identity of entities or specific locations of assets, either because such information was not submitted to the E-ISAC or because the E-ISAC has removed such information. Protected Information may be submitted by entities concerning facilities both within and outside of the BPS as well as by entities that are not NERC registered entities.
>
> Information that is reported to any other NERC department or to the government is not Protected Information for the purposes of this E-ISAC Code of Conduct. However, all NERC employees, including E-ISAC

The Code of Conduct provides only limited exceptions to this rule. Specifically, the E-ISAC may share Attributed Protected Information only with (1) NERC's president and CEO for providing oversight of the E-ISAC; (2) NERC's General Counsel for providing legal advice to NERC, (3) other persons or entities with whom the submitting entity has provided permission prior to any such sharing, and (4) those persons and entities authorized to review such information pursuant to policies approved by the ESCC. NERC's Bulk Power System Awareness ("BPSA") Department personnel may receive Unattributed Protected Information to support situational awareness. The Code of Conduct does not allow the E-ISAC to share Attributed or Unattributed Protected Information with the Standards Department or any other program area.[37]

Despite these restrictions, NERC may use certain E-ISAC data to inform Reliability Standard development activities. The Standards Department looks at all available public information, including publicly available information provided by the E-ISAC, to incorporate cybersecurity awareness into Standards. The E-ISAC may share with other NERC program areas any of its public or non-public reports that anonymize and aggregate Protected Information. Such reports would include, for example, trending analysis or analysis of a specific threat, vulnerability,

---

personnel, are nonetheless governed by this Code of Conduct at all times. Information that is not Protected Information under this Code of Conduct is subject to any applicable confidentiality policies that apply to such information and to all NERC employees.

The following information is specifically identified as not constituting Protected Information for purposes of this Code of Conduct:

(i) Information mandated by NERC Reliability Standards or other applicable governmental authority's laws, rules, regulations, or orders;

(ii) Information required by Department of Energy Form OE-417, NERC EOP-004 reports, and Federal Energy Regulatory Commission Order Nos. 693, 706, and 761;

(iii) Information voluntarily provided to NERC through the Event Analysis (EA) program;

(iv) Information that is discovered or reported pursuant to a compliance monitoring method (whether self-identified or externally identified) set forth in the CMEP; or

(v) Information that is otherwise publicly available or simultaneously reported to another NERC department.

[37] E-ISAC Code of Conduct, at Sections 4 and 5.

or risk that does not implicate an incident at a specific member or entity. The E-ISAC may also share with the Standards Department any mandatory reports submitted to the E-ISAC in accordance with the CIP-008 Reliability Standard.

Consistent with the E-ISAC Code of Conduct, NERC currently may access certain of the reports issued by the E-ISAC to help inform standards development, where appropriate. These reports summarize data from the E-ISAC's various data streams and include aggregated and anonymized information only. NERC also makes E-ISAC personnel available as subject matter experts for consultation with Standards Department staff and drafting teams as circumstances warrant.

NERC plans to enhance the E-ISAC's coordination with the Standards Department by relying on permissible forms of information sharing and increasing the knowledge exchange between subject matter experts in the E-ISAC and the ERO Enterprise. NERC will initiate quarterly meetings between the E-ISAC and Standards Department personnel to discuss E-ISAC information that could help inform standards development activities, to the extent permitted by the E-ISAC Code of Conduct. This would establish a regular feedback loop between these program areas.

NERC also commits to establish a process whereby Standards Department personnel and ERO Enterprise subject matter experts for the Critical Infrastructure Protection ("CIP") Reliability Standards review E-ISAC information, subject to E-ISAC Code of Conduct restrictions, to perform reliability gap analysis. If staff identifies a potential gap in Reliability Standards, NERC would then either informally review the matter with industry to gather more information or initiate a Standard Authorization Request. These efforts would include, for example, coordination with the RSTC and its subgroups, as appropriate. Finally, NERC will continue to make E-ISAC personnel

available as subject matter experts for consultation with Standards Department staff and drafting teams as circumstances warrant.

B. NERC's Relationship with the Electricity Subsector Coordinating Council Member Executive Committee

In its Order, the Commission also requested that NERC provide additional information to clarify the relationship between the E-ISAC and the ESCC's MEC. In particular, the Commission directed NERC to "describe how the MEC provides 'strategic oversight and guidance' to guide and support the E-ISAC… as well as what other aspects of the E-ISAC, if any, the MEC is responsible for approving."[38]

As discussed below, the MEC is an advisory body to the E-ISAC, providing industry support and strategic guidance to NERC on the E-ISAC's short- and long-term vision, operational focus areas, budget development, and performance metrics, among other matters. While prior NERC filings may have used different language to describe the MEC, its overall objective is to provide senior industry leadership expertise and guidance to help set the strategic direction of the E-ISAC and increase its value to the electricity sector. The MEC serves in an advisory capacity only. NERC retains sole responsibility for the management and operation of the E-ISAC. In its capacity as an advisory body, the MEC may propose that the E-ISAC take certain action and may participate in the development of and vote to endorse the proposed E-ISAC budget, the E-ISAC Long-Term Strategic Plan, and the E-ISAC's performance metrics, but it does not have a formal role in approving those items. It is the responsibility of the NERC Board to accept or approve those items and for NERC management to implement them. The following discussion provides

[38] Order, *supra*, at P 70.

additional background on the establishment of the MEC and the manner in which it supports NERC's operation of the E-ISAC.

The ESCC established the MEC following the ESCC's Strategic Review of the E-ISAC in 2015.[39] Recognizing the criticality of sharing cyber and physical security information across the electricity sector and the role of the E-ISAC in facilitating such information exchange, the ESCC performed a review of the E-ISAC to enhance its effectiveness and increase its value to the electricity sector. During its Strategic Review, the ESCC examined critical infrastructure owners' and operators' use of the E-ISAC to identify, understand, and clarify the challenges and opportunities to strengthening the effectiveness of information sharing within the sector. Among other things, the Strategic Review team evaluated E-ISAC products and services and sought to identify where the E-ISAC should focus resources moving forward.

The Strategic Review team issued several recommendations adopted by the ESCC with the aim of assisting the E-ISAC in creating a path forward. A central recommendation of the Strategic Review was to establish the MEC to increase stakeholder engagement and provide senior industry leadership and expertise to guide and support the E-ISAC. The ESCC recognized that strong industry support from executive-level personnel was an important step to increasing the level of information sharing across the industry and enhancing the value of the E-ISAC. To that end, the

[39] The ESCC's Strategic Review was supported by NERC Management. NERC's President and CEO at the time served as one of the ESCC sponsors of the Strategic Review. As reflected in the minutes of their August 2015 meeting, the NERC Board was also supportive of the Strategic Review and the establishment of the MEC. The NERC Board issued a resolution at that meeting to, among other things, acknowledge its support of the Strategic Review and the MEC, direct NERC management to actively engage with the MEC, and request an amendment to the MEC charter to recognize the NERC Board's legal and fiduciary role with respect to the E-ISAC. The ESCC revised the MEC charter consistent with the NERC Board's request. The minutes for the NERC Board's August 2015 meeting are available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20August%2013%202015%20Minutes.pdf#search=%22Strategic%20Review%22.

MEC's charter provides that the MEC must be comprised of executives across the industry.[40] The MEC is currently chaired by two industry CEOs that are members of the ESCC. The remaining members are Chief Security Officers, Chief Information Officers, or equivalent positions at E-ISAC member companies, as well as the NERC CEO. The members represent companies from various segments of the industry and are diverse in their ownership and geography.

As provided in the MEC charter, the ESCC charged the MEC with providing industry leadership and strategic direction to the E-ISAC by supporting the E-ISAC in carrying out the following activities, among others:

- Developing the short- and long-term strategic vision of the E-ISAC.[41]
- Defining and maintaining a business strategy to provide necessary and appropriate products and services to E-ISAC members.
- Setting goals for E-ISAC operations, capabilities, and controls.
- Developing policies and providing guidance regarding the protection and dissemination of confidential information.
- Developing the E-ISAC budget, including appropriate staffing levels.

Recognizing the role and responsibilities of NERC management in the day-to-day operation and management of the E-ISAC and the NERC Board's responsibilities for overseeing the E-ISAC, the ESCC established the MEC as an advisory committee. The MEC's role is to provide strategic-level guidance, not to provide day-to-day oversight or management of the E-

[40] The charter specifies that the MEC shall be comprised of 11 members that meet one of the following criteria: (1) a CEO-level executive from an E-ISAC member organization; (2) an executive (no less than vice president-level) from an E-ISAC member organization with responsibility regarding information technology and security (e.g., Chief Information Officers, Chief Information Security Officers, or Chief Technology Officers); or (3) a subject matter expert sponsored by an E-ISAC member organization with certified or substantial expertise in the area of information technology, security or law.

[41] The MEC played a pivotal role in assisting the E-ISAC in developing the E-ISAC Long-Term Strategic Plan. At its August 2016 meeting, the NERC Board specifically requested that NERC management work with the ESCC and the MEC to develop a five-year strategic plan that would allow the Board to consider the overall implications of the development of the E-ISAC.

ISAC. The MEC does not have a formal role in approving the E-ISAC Long-Term Strategic Plan, the E-ISAC budget, the E-ISAC's performance metrics, or other actions the E-ISAC may take to fulfill its mission. Instead, for items like the Long-Term Strategic Plan, the annual E-ISAC Budget, or the E-ISAC performance metrics, the MEC will provide guidance on their development and, where appropriate, vote to endorse these items to indicate its support for the items to NERC management and the NERC Board.[42]

While the MEC may propose the E-ISAC take certain action and vote to endorse certain items, it is ultimately the responsibility of the NERC Board to accept or approve those items and for NERC management to implement them. The ESCC's and the MEC's expectation is that NERC management and the NERC Board give due consideration to the MEC's proposals and endorsements within the context of fulfilling its legal and fiduciary obligations.

The strategic direction and guidance provided to by the MEC has played a pivotal role in the E-ISAC's enhanced operational capabilities and expanded use among electricity infrastructure owners and operators. In fulfilling their respective roles overseeing and managing the E-ISAC, the NERC Board, and NERC management give significant weight to the guidance provided by the MEC. The MEC meets on a quarterly basis with representatives of NERC management, E-ISAC personnel, and a NERC Board member to discuss the E-ISAC's strategic direction and operational focus areas, and to identify opportunities and challenges to enhance the E-ISAC's information sharing and analysis capabilities, among other things. These meetings occur in advance of the

[42] In the Order, the Commission cites to NERC's 2020 business plan and budget filing, which stated that the MEC "approved" the E-ISAC Long-Term Strategic Plan. That filing used the wrong term. As reflected in the minutes of the NERC Board for its May 11, 2017 meeting, the MEC actually voted to "endorse" the E-ISAC Long-Term Strategic Plan. The NERC Board minutes are available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20May%2011%202017%20Minutes.pdf.

NERC quarterly Board meetings where the E-ISAC provides an overview of the MEC meeting to the NERC Board's Technology and Security Committee ("BOTTSC") at its open meeting. The E-ISAC's presentations to the BOTTSC and the BOTTSC minutes are publicly available should the Commission seek additional information on the items with which the MEC is currently focused.[43]

C. E-ISAC Performance Metrics

The Commission also directed NERC to provide additional information regarding the performance metrics NERC uses to assess the effectiveness of the E-ISAC. Specifically, the Commission directed that NERC:

> include in the ninety (90) day compliance filing the E-ISAC metrics for FY 2020 discussing: (1) the scope and basis used for developing those metrics; (2) how the metrics assist NERC in its oversight responsibility of the E-ISAC; (3) how the metrics were developed; and (4) how those metrics and goals are relevant to the E-ISAC's mission.[44]

As stated in the Performance Assessment, the E-ISAC developed a set of performance metrics for 2020 as a tool to help measure its effectiveness and its progress against its Long-Term Strategic Plan. The MEC provided input into the development of those metrics and endorsed them at its October 2019 meeting. The E-ISAC publicly presented the proposed metrics at the November 2019 open meeting of the BOTTSC, which voted to accept those metrics as presented.[45] NERC incorporated the E-ISAC 2020 performance metrics into its 2020 Work Plan Priorities, which the

---

[43] The E-ISAC's presentations to the BOTTSC and the BOTTSC minutes are publicly available at https://www.nerc.com/gov/bot/bottsc/Pages/TechnologyandSecurityCommittee.aspx.

[44] Order, *supra*, at P 72.

[45] The metrics and the BOTTSC's minutes from its November 2019 meeting reflecting the BOTTSC acceptance of those metrics are publicly available at https://www.nerc.com/gov/bot/bottsc/Pages/TechnologyandSecurityCommittee.aspx.

NERC Board accepted at its February 2020 meeting.[46] The following section provides additional detail on each item the Commission mentioned in its directive.

1. Scope and Basis for Developing Metrics

The E-ISAC developed its 2020 performance metrics in response to discussions with the MEC, other stakeholders, NERC management, and the NERC Board regarding the need to develop mechanisms to assess the E-ISAC's performance, value to industry, and effect on the security of the North American grid. The ultimate objective of the E-ISAC′s metrics, as with any set of metrics, is to identify opportunities for improvement and areas in which the E-ISAC could increase value for stakeholders.

For 2020, the scope of the E-ISAC's metrics is measuring the E-ISAC's performance against the E-ISAC Long-Term Strategic Plan and its effectiveness in carrying out the key activities underlying the plan. The 2020 metrics focus on the three pillars of the E-ISAC's Long-Term Strategic Plan: engagement, information sharing, and analysis.

For engagement, the metrics are focused primarily on building and enriching E-ISAC membership and engagement levels and strengthening trusted-source partnerships (e.g., with government agencies, vendors, and other ISACs). To that end, the engagement metrics seek to measure, among other things: (1) the increase in the number of organizations with portal accounts; (2) the level of engagement with those members; and (3) participation in GridEx and other E-ISAC programs.

For information sharing, the 2020 metrics are focused primarily on increasing information sharing by industry participants and trusted partners, as well as improving the E-ISAC sharing of

[46] The NERC Board's Corporate Governance and Human Resource Committee ("CGHRC") oversees all of NERC's metrics and Work Plan Priorities. At its meeting in February 2020, the CGHRC recommended that the NERC Board accept the 2020 Work Plan Priorities.

value-added, actionable information to industry and trusted partners. To that end, the information sharing metrics measure, among other things, the level of information sharing by asset owners and operators, trusted partners, and the E-ISAC, looking at when, how, and what information is being shared.

For analysis, the 2020 metrics are focused primarily on strengthening the E-ISAC's analytical capabilities through the development and use of new data sources, analytical tools, and capabilities. To that end, the analysis metrics measure, among other things, the increase of content enriched by E-ISAC analysis and analytical products.

The 2020 E-ISAC performance metrics are designed to set an initial baseline of data and items the E-ISAC will use to track and evaluate its performance in its key focus areas. In future years, the E-ISAC expects to evolve the metrics over time to be a mix of quantitative and qualitative measurements as its processes and data sources mature. The E-ISAC will consider ways to expand the metrics not only to measure the E-ISAC's effectiveness in performing its activities under the plan but also, where possible, to measure the E-ISAC's impact on the electric industry. For instance, as the E-ISAC develops mature feedback processes with its members, it may be able to begin measuring the manner in which information sharing in general, and specific pieces of information (delivered through a NERC Alert or other forms of communication) in particular, changes the security posture or practices of its members and industry at large.

2. Assistance with NERC Oversight Responsibility

In addition to allowing the E-ISAC staff to identify opportunities for improvement and understand ways to enhance its value to stakeholders, the E-ISAC performance metrics will allow NERC management and its Board to enhance its oversight of the E-ISAC. As noted in the Performance Assessment, the E-ISAC plans to provide quarterly metrics reports to the MEC and

to the NERC Board, which could occur both at the BOTTSC and as part of the quarterly updates on NERC's progress against 2020 Work Plan Priorities. By measuring the E-ISAC's performance in specific areas over time, NERC strategic decisions and the manner in which resources are allocated within the E-ISAC will be more informed. The ultimate objective of the metrics and NERC's oversight is to help ensure that the E-ISAC is continually working to enhance its value to industry.

3. Metrics Development

As noted in the Performance Assessment, the E-ISAC developed the metrics in consultation with the MEC. In developing the metrics, the E-ISAC considered available data sources, available historical information baselines, functional units responsible for the performance of each metric, the proper calculations and underlying definitions for the items being measured, and the feasibility of measurement in 2020. As noted, as the E-ISAC gets the baseline data from the 2020 metrics and matures its tools and capabilities for capturing additional data sets, the E-ISAC expects to enhance the focus and granularity of its metrics. As it enhances its set of metrics, the E-ISAC will assess the cost and practicality of each metric relative to the benefit of or the risk mitigated by that measurement.

4. Relevance of Metrics and Goals to the E-ISAC's Mission

As noted above, the E-ISAC designed its metrics to align with the goals and key activities of, and to measure the E-ISAC's performance against, its Long-Term Strategic Plan. As the Long-Term Strategic Plan is designed specifically to help the E-ISAC achieve its mission, the metrics will ultimately help NERC measure the E-ISAC's performance in achieving its mission.

IV. Update Regarding Revisions to the Rules of Procedure

In addition to the clarifications provided in this compliance filing, NERC confirms that it remains on schedule to submit revisions to its ROP that conform with the enhancements directed by the Commission's Order. NERC has prepared revisions to its rules regarding the Sanction Guidelines, Certification process, and E-ISAC, as well as other improvements that NERC had been developing prior to the Order. These proposals have been posted on NERC's website for public comment. NERC will submit these revisions on or before September 28, 2020.

V. Conclusion

Wherefore, for the foregoing reasons, NERC respectfully requests that the Commission accept this compliance filing as responsive to the directives in the Order.

Respectfully submitted,

/s/ Nina H. Jenkins-Johnston

Nina H. Jenkins-Johnston
Senior Counsel
Shamai Elstein
Assistant General Counsel
Candice Castaneda
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
nina.johnston@nerc.net
shamai.elstein@nerc.net
candice.castaneda@nerc.net

Counsel for North American Electric Reliability Corporation

Date: June 1, 2020

PUBLIC VERSION
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED PURSUANT TO 18 C.F.R. § 388.112

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding. Dated at Washington, D.C. this 1st day of June 2020.

/s/ Nina H. Jenkins-Johnston

Nina H. Jenkins-Johnston

Senior Counsel for North American Electric Reliability Corporation

Attachment 1

Proposed Model Form of Protective Agreement

PUBLIC VERSION
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED PURSUANT TO 18 C.F.R. § 388.112

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RR19-7-001**

PROTECTIVE AGREEMENT

1. This Protective Agreement shall govern the use of all Protected Materials produced by, or on behalf of, any Participant. Notwithstanding any order terminating this proceeding, this Protective Agreement shall remain in effect until specifically modified or terminated by the Federal Energy Regulatory Commission (the "Commission") or the Presiding Administrative Law Judge, if one shall be designated ("Presiding Judge") (which includes the Chief Administrative Law Judge).

2. This Protective Agreement applies to the following two categories of materials: (A) a Participant may designate as protected those materials which customarily are treated by that Participant as sensitive or proprietary, which are not available to the public, and which, if disclosed freely, would subject that Participant or its customers to risk of competitive disadvantage or other business injury; and (B) a Participant shall designate as protected those materials which contain critical energy infrastructure information, as defined in 18 C.F.R. § 388.113(c)(1) ("Critical Energy Infrastructure Information").

3. Definitions – For purposes of this Protective Agreement:

4. The term "Participant" shall mean a Participant as defined in 18 C.F.R. § 385.102(b) in the above dockets.

5. The term "Protected Materials" means (A) materials filed by a Participant and designated as protected; (B) materials (including depositions) provided by a Participant in response to discovery requests and designated by such Participant as protected; (C) any information contained in or obtained from such designated materials; (D) any other materials which are made subject to this Protective Agreement by the Commission, by any court or other body having appropriate authority, or by agreement of the Participants;

(E) notes of Protected Materials; and (F) copies of Protected Materials. The Participant producing the Protected Materials shall physically mark them on each page as "**PROTECTED MATERIALS PROVIDED PURSUANT TO PROTECTIVE AGREEMENT**" and "**DO NOT RELEASE**," or with words of similar import as long as the term "Protected Materials" is included in that designation to indicate that they are Protected Materials. In addition:

a. If the Protected Materials contain Critical Energy Infrastructure Information, the Participant producing such information shall additionally mark on each page of the document containing such information the words "**CUI//PRIV/CEII**."
b. If the Protected Materials contain information that is privileged but is not categorized as Critical Energy Infrastructure Information, the Participant producing such information shall additionally mark on each page of the document containing such information the words "**CUI//PRIV**."

6. The term "Notes of Protected Materials" means memoranda, handwritten notes, or any other form of information (including electronic form) which copies or discloses materials described in Paragraph 5. Notes of Protected Materials are subject to the same restrictions provided in this Protective Agreement for Protected Materials except as specifically provided in this Protective Agreement.

7. Protected Materials shall not include (A) any information or document contained in the files of the Commission (unless the information or documents were submitted to the Commission subject to an express or implied request for privileged treatment pursuant to 18 C.F.R. § 388.112, and such information or documents is accorded privileged treatment by the Commission), or any other federal or state agency, or any federal or state court, unless the information or document has been determined to be protected by such agency or court, (B) information that is public knowledge, or which becomes public knowledge, other than through disclosure in violation of this Protective Agreement, or (C) any information or document labeled as "Non-Internet Public" by a Participant, or in accordance with Paragraph 30 of FERC Order No. 630, FERC Stats. & Regs. ¶ 31,140. Protected Materials do include any information or document contained in the files of the Commission that has been designated as Critical Energy Infrastructure Information.

8. Non-Disclosure Certificates

   The term "Non-Disclosure Certificate" shall mean the certificate annexed hereto by which Participants who have been granted access to Protected Materials shall certify their understanding that such access to Protected Materials is provided pursuant to the terms and restrictions of this Protective Agreement, and that such Participants have read the

Protective Agreement and agree to be bound by it. All Non-Disclosure Certificates shall be served on all parties on the official service list maintained by the Secretary in this proceeding.

9. The term "Reviewing Representative" shall mean a person who has signed a Non Disclosure Certificate and who is:
    a. An attorney who has made an appearance in this proceeding for a Participant;
    b. Attorneys, paralegals, and other employees associated for purposes of this case with an attorney described in Paragraph 9(a)(1);
    c. An expert or an employee of an expert retained by a Participant for the purpose of advising, preparing for or testifying in this proceeding;
    d. A person designated as a Reviewing Representative by order of the Commission;
    e. Employees or other representatives of Participants appearing in this proceeding with significant responsibility for this docket; or
    f. Commission Trial Staff designated as such in this proceeding.

10. Protected Materials shall be made available under the terms of this Protective Agreement only to Participants and only through their Reviewing Representatives.

11. Protected Materials shall remain available to Participants until the later of the date that an order terminating this proceeding becomes no longer subject to judicial review, or the date that any other Commission proceeding relating to the Protected Materials is concluded and no longer subject to judicial review. If requested to do so in writing after that date, the Participants shall, within fifteen days of such request, return the Protected Materials (excluding Notes of Protected Materials) to the Participant that produced them, or shall destroy the materials, except that copies of filings, official transcripts, and exhibits in this proceeding that contain Protected Materials, and Notes of Protected Material may be retained, if they are maintained in accordance with Paragraphs 12 and 13. Within such time period each Participant, if requested to do so, shall also submit to the producing Participant an affidavit stating that, to the best of its knowledge, all Protected Materials and all Notes of Protected Materials have been returned or have been destroyed or will be maintained in accordance with Paragraphs 12 and 13. To the extent Protected Materials are not returned or destroyed, they shall remain subject to the Protective Agreement.

12. All Protected Materials shall be maintained by the Participant in a secure place. Access to those materials shall be limited to those Reviewing Representatives specifically authorized pursuant to Paragraphs 14 and 15. The Secretary will place any Protected Materials filed with the Commission in a non-public file. By placing such documents in a non-public file, the Commission is not making a determination of any claim of privilege.

The Commission retains the right to make determinations regarding any claim of privilege and the discretion to release information necessary to carry out its jurisdictional responsibilities.

13. For documents submitted to Commission Staff ("Staff"), Staff shall follow the notification procedures of 18 C.F.R. § 388.112 before making public any Protected Materials.

14. Protected Materials shall be treated as confidential by each Participant and by the Reviewing Representative in accordance with the Non-Disclosure Certificate executed pursuant to Paragraph 17. Protected Materials shall not be used except as necessary for the conduct of this proceeding, nor shall they be disclosed in any manner to any person except a Reviewing Representative who is engaged in the conduct of this proceeding and who needs to know the information in order to carry out that person's responsibilities in this proceeding. Reviewing Representatives may make copies of Protected Materials, but such copies become Protected Materials. Reviewing Representatives may make notes of Protected Materials, which shall be treated as Notes of Protected Materials if they disclose the contents of Protected Materials.

15. If a Reviewing Representative's scope of employment includes the marketing of energy or generation assets, the direct supervision of any employee or employees whose duties include the marketing of energy or generation assets, the provision of consulting services to any person whose duties include the marketing of energy or generation assets, or the direct supervision of any employee or employees whose duties include the marketing of energy or generation assets, such Reviewing Representative may not use information contained in any Protected Materials obtained through this proceeding to give any Participant or any competitor of any Participant a commercial advantage.

16. In the event that a Participant wishes to designate as a Reviewing Representative a person not described in Paragraph 9, the Participant shall seek agreement from the Participant providing the Protected Materials. If an agreement is reached, that person shall be a Reviewing Representative pursuant to Paragraph 9 with respect to those materials. If no agreement is reached, the Participant shall submit the disputed designation to the Commission for resolution.

17. A Reviewing Representative shall not be permitted to inspect, participate in discussions regarding, or otherwise be permitted access to Protected Materials pursuant to this Protective Agreement unless that Reviewing Representative has first executed a NonDisclosure Certificate or; provided that if an attorney qualified as a Reviewing Representative has executed such a certificate, the paralegals, secretarial, and clerical

personnel employed by the same entity as the attorney and under the attorney's instruction, supervision, or control need not do so. A copy of each Non-Disclosure Certificate and NonDisclosure Certificate for Competitive Duty Personnel shall be provided to counsel for the Participant asserting confidentiality prior to disclosure of any Protected Material to that Reviewing Representative.

18. Attorneys qualified as Reviewing Representatives are responsible for ensuring that persons under their supervision or control comply with this order.

19. Any Reviewing Representative may disclose Protected Materials to any other Reviewing Representative entitled to receive the specific category of Protected Materials under Paragraph 5, as long as the disclosing Reviewing Representative and the receiving Reviewing Representative both have executed a Non-Disclosure Certificate. In the event that any Reviewing Representative to whom the Protected Materials are disclosed ceases to be engaged in these proceedings, or is employed or retained for a position whose occupant is not qualified to be a Reviewing Representative under Paragraph 9, access to Protected Materials by that person shall be terminated. Even if no longer engaged in this proceeding, every person who has executed a Non-Disclosure Certificate shall continue to be bound by the provisions of this Protective Agreement and the certification.

20. Subject to Paragraph 27, the Commission or Presiding Judge shall resolve any disputes arising under this Protective Agreement. Prior to presenting any dispute under this Protective Agreement to the Commission or Presiding Judge, as appropriate, the parties to the dispute shall use their best efforts to resolve it. Any Participant that contests the designation of materials as protected shall notify the party that provided the Protected Materials by specifying in writing the materials whose designation is contested. This Protective Agreement shall automatically cease to apply to such materials fifteen business days after the notification is made unless the designator, within said fifteen-day period, files a motion with the Commission or Presiding Judge, with supporting affidavits, demonstrating that the materials should continue to be protected. In any challenge to the designation of materials as protected, the burden of proof shall be on the Participant seeking protection. If the Commission or Presiding Judge finds that the materials at issue are not entitled to protection, the procedures of Paragraph 27 shall apply. The procedures described above shall not apply to Protected Materials designated by a Participant as Critical Energy Infrastructure Information. Materials so designated shall remain protected and subject to the provisions of this Protective Agreement, unless a Participant requests and obtains a determination from the Commission's Critical Energy Infrastructure Information Coordinator that such materials need not remain protected.

21. Unless filed or served electronically, all copies of all documents reflecting Protected Materials, including the portion of other documents which refer to Protected Materials, shall be filed and served in sealed envelopes or other appropriate containers endorsed to the effect that they are sealed pursuant to this Protective Agreement. Such documents shall be marked "**PROTECTED MATERIALS PROVIDED PURSUANT TO PROTECTIVE AGREEMENT**" (or words of similar import) with the appropriate designation (as relevant) under Paragraph 5 and shall be filed under seal and served under seal upon the Commission and all Reviewing Representatives who are on the service list. Such documents containing Critical Energy Infrastructure Information shall be additionally marked "Contains Critical Energy Infrastructure Information – Do Not Release." For anything filed under seal, redacted versions or, where an entire document is protected, a letter indicating such will also be filed with the Commission and served on all parties on the service list. Counsel for the producing Participant shall provide to all Participants who request the same, a list of Reviewing Representatives who are entitled to receive such material. Counsel shall take all reasonable precautions necessary to assure that Protected Materials are not distributed to unauthorized persons.

22. If any Participant desires to include, utilize, or refer to any Protected Materials or information derived there from in testimony or exhibits in these proceedings in such a manner that might require disclosure of such material to persons other than Reviewing Representatives, such Participant shall first notify both counsel for the disclosing participant and the Commission of such desire, identifying with particularity each of the Protected Materials. Thereafter, use of such Protected Material will be governed by procedures determined by the Commission.

23. Nothing in this Protective Agreement shall be construed as precluding any Participant from objecting to the use of Protected Materials on any legal grounds.

24. Nothing in this Protective Agreement shall preclude any Participant from requesting the Commission or Presiding Judge, or any other body having appropriate authority, to find that this Protective Agreement should not apply to all or any materials previously designated as Protected Materials pursuant to this Protective Agreement. The Commission or Presiding Judge, as appropriate, may alter or amend this Protective Agreement as circumstances warrant at any time during the course of this proceeding after appropriate notice and opportunity for a hearing on the alteration or amendment.

25. Each party governed by this Protective Agreement has the right to seek changes in it as appropriate from the Commission or Presiding Judge.

26. Unless filed or served electronically, all Protected Materials filed with the Commission, or any other judicial or administrative body, in support of, or as a part of, a motion, other pleading, brief, or other document, shall be filed and served in sealed envelopes or other appropriate containers bearing prominent markings indicating that the contents include Protected Materials subject to this Protective Agreement and with the appropriate designation (as relevant) under Paragraph 5. Such documents containing Critical Energy Infrastructure Information shall be additionally marked "Contains Critical Energy Infrastructure Information – Do Not Release."

27. If the Commission or a Presiding Judge finds at any time in the course of this proceeding that all or part of the Protected Materials need not be protected, those materials shall, nevertheless, be subject to the protection afforded by this Protective Agreement for a time period designated by the Commission or Presiding Judge, but not less than fifteen business days from the date of issuance of the Commission's or Presiding Judge's decision. None of the Participants waives its rights to seek additional administrative or judicial remedies after the Commission's or Presiding Judge's decision respecting Protected Materials or Reviewing Representatives, or the Commission's or Presiding Judge's denial of any appeal thereof. The provisions of 18 C.F.R. § 388.112 shall apply to any requests for Protected Materials in the files of the Commission under the Freedom of Information Act (5 U.S.C. § 552).

28. Nothing in this Protective Agreement shall be deemed to preclude any Participant from independently seeking through discovery in any other administrative or judicial proceeding information or materials produced in this proceeding under this Protective Agreement.

29. None of the Participants waives the right to pursue any other legal or equitable remedies that may be available in the event of actual or anticipated disclosure of Protected Materials.

30. The contents of Protected Materials or any other form of information that copies or discloses Protected Materials shall not be disclosed to anyone other than in accordance with this Protective Agreement and shall be used only in connection with this proceeding.

The undersigned Participants hereby agree to the foregoing terms of this Protective Agreement.

By:

_____

Printed Name:

_____

Title:

_____

Representing:

_____

Date: _____

Attachment 2

Audits of Regional Entities during the Assessment Period