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 COMPLIANCE FILINGS

Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

June 30, 2023

TABLE OF CONTENTS

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 COMPLIANCE FILINGS

The North American Electric Reliability Corporation ("NERC") hereby submits this compliance filing in accordance with the Federal Energy Regulatory Commission's ("FERC" or the "Commission") January 19, 2021 Order ("Order on Compliance Filings"),[1] issued in the five-year NERC Performance Assessment docket, directing NERC to submit reports for audits of all six Regional Entities pursuant to NERC Rules of Procedure ("ROP") Appendix 4A by June 30, 2023.[2] NERC requests that the Commission accept this compliance filing in satisfaction of this directive and NERC's obligation in ROP Section 402.1.3 to submit such audit reports to Applicable Governmental Authorities.[3] This filing covers the audit period of January 1, 2020 to December 31, 2021.

This compliance filing is organized as follows: Section I provides a high level summary of the key takeaways from this filing including an overview of the vision for the ERO Enterprise's risk-based Compliance Monitoring and Enforcement Program ("CMEP"). Section II provides an

---

1 *N. Am. Elec. Reliability Corp.*, Order on Compliance Filings, 174 FERC ¶ 61,030 at P 22 (2021).

2 Pursuant to FERC's regulations at 18 C.F.R. § 39.3(c) (2023) and the directives in Order No. 672, NERC must submit a report that it continues to meet ERO certification criteria. NERC, *NERC Five-Year Electric Reliability Organization Performance Assessment Report in Accordance with 18 C.F.R. § 39.3(c)*, Docket No. RR19-7-000 (July 22, 2019).

3 Unless otherwise designated, all capitalized terms shall have the meaning set forth in Appendix 2 to the NERC ROP, available at https://www.nerc.com/AboutNERC/RulesOfProcedure/ROP_Appendix%202_20220519.pdf.

overview of the tasks NERC and the Regional Entities will perform, called Management Action Plans ("MAPs"), to implement the improvement opportunities and observations identified by NERC's Internal Audit ("IA") function. Section III describes the Appendix 4A audit engagements, including the audit team composition, audit objective, audit scope, and observations. Finally, Section IV concludes the filing. **Attachments A-G** include a summary of audit observations and audit reports for each of the six Regional Entities.[4]

I. SUMMARY

A key part of NERC's implementation of the CMEP is the ability to independently assess the effectiveness of the risk-based CMEP. To that end, NERC IA focuses on this objective in its audit activities of the CMEP. One such means of executing this role is through an audit program pursuant to ROP 402.1.3 and Appendix 4A. This audit occurs at least once every five years. It examines the six Regional Entities' compliance with the ROP and its Appendix 4C, Regional Delegation Agreements and any directives in effect pursuant to those agreements, the annual ERO CMEP Implementation Plan ("IP"), required CMEP attributes, and NERC CMEP guidance and procedures. NERC provides such audit reports to Applicable Governmental Authorities.

At the conclusion of its audits, NERC IA found that the Regional Entities continue to be capable of performing duties under the ROP as well as the Regional Delegation Agreements and that there were no significant instances of noncompliance. During the course of the evaluation, several best practices, such as the development and implementation of automated tools across certain of the Regional Entities, were identified that augment the CMEP processes across the

[4] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council. Collectively, NERC and the Regional Entities are known as the Electric Reliability Organization ("ERO") Enterprise.

Regional Entities. These best practices are attributed to strong leadership and focus on optimal organizational structure, subject matter expertise, and innovation.

In addition, NERC IA identified opportunities for improvement in the evolution of the ERO Enterprise's risk-based approach. In particular, NERC IA identified the opportunity to improve NERC oversight activities to drive greater adoption of risk-based methodologies, further harmonize processes, and more effectively use monitoring tools across the ERO Enterprise. With the support of NERC oversight, the Regional Entities will continue to move to a holistic framework that includes ongoing assessments of all registered entities based on their assets and risk to the Bulk-Power System ("BPS") rather than focusing mostly on registered entities with functions subject to a three-year audit requirement under the ROP. This will enable Regional Entities to achieve greater balance in the use of monitoring tools and bolster the rationale for monitoring intervals of registered entities.

To that end, NERC CMEP leadership is focusing its near-term efforts on program development to guide the Regional Entities in aligning their use of CMEP tools and processes. Risk-based CMEP activities will include more comprehensive and dynamic monitoring that is risk-informed and aligned with leading auditing practices. The ERO Enterprise's implementation of Align, a single, secure platform for the core CMEP business processes of NERC and the Regional Entities, made significant progress in consistency across Regional Entities, and now that it is implemented, the ERO Enterprise's resources can fully focus on program development going forward.

NERC IA will continue to monitor these efforts through its periodic risk assessment process as well as any targeted audits warranted under its annual audit plan, which is approved by the NERC Board of Trustees Finance and Audit Committee ("FAC"). NERC CMEP leadership

will leverage ERO Enterprise collaboration groups composed of Regional Entity management and program area leaders to work on program development. These efforts are separate and distinct from NERC's oversight activities but support consistency and effectiveness of the CMEP across the ERO Enterprise since all six Regional Entities participate in these collaboration groups.

In addition to program development, the NERC CMEP will enhance its oversight, including support of training exercises to facilitate more robust and consistent implementation of risk-based practices. The oversight strategy will focus on setting clear expectations for CMEP implementation. Various factors inform this oversight strategy, including independent audit results conducted by NERC IA, results from previous oversight activities, measures tracked through program development, and industry perception or feedback. The program development activities will also inform NERC's oversight strategy.

II. ERO ENTERPRISE CMEP PROGRAM DEVELOPMENT

NERC, in coordination with the Regional Entities, will focus on program development to further improve consistency of CMEP implementation. As part of this program development, NERC and the Regional Entities identified tasks in response to NERC IA recommendations resulting from the audits conducted pursuant to NERC ROP Appendix 4A, which are described in more detail in Section III below and **Attachments A-G**. NERC and the Regional Entities call these tasks Management Action Plans. Regional Entities developed MAPs to ensure program activities and requirements are addressed and are effectively implemented. In addition, NERC CMEP leadership developed MAPs related to its oversight in response to the Appendix 4A audits even though NERC was not a subject of the audits.[5]

[5] NERC's own performance was the subject of a separate audit. At least every three years, the NERC CMEP must undergo an independent audit performed under ROP Section 406. The 2022 Section 406 CMEP audit report is available at https://www.nerc.com/gov/bot/ERC/relateddocs/NERC%20CMEP%20audit%20report_FINAL_011223_PR.pdf.

An effective internal audit program must have a process for following up on and monitoring the status of corrective actions undertaken by management to address observations and recommendations identified during audit engagements and communicated to business area management.[6] To that end, NERC IA has communicated recommendations to improve upon areas identified in observations. While each Regional Entity audit report includes specific MAPs and individuals responsible for each MAP in **Attachments B-G**, NERC IA also developed recommendations for NERC staff as a result of the Appendix 4A audits that complement the Regional Entity MAPs to help achieve effective implementation of the CMEP, available in **Attachment A**. The observations from the Appendix 4A audit engagements relate to enhancements of NERC CMEP oversight activities to: (1) continue to drive greater adoption of a risk-based methodology, (2) further harmonize CMEP processes, and (3) increase effective use of monitoring tools across the ERO Enterprise.

NERC IA will continue to perform the follow up process to track completion of MAPs for all Regional Entities. Once the MAPs have been completed, NERC IA will evaluate the effectiveness of the implemented MAPs. NERC IA will also conduct the same follow up process for NERC MAPs that are designed to improve oversight of the Regional Entities. NERC IA will then perform periodic risk assessments quarterly, at a minimum, to identify and monitor risks to the CMEP. These risk assessments will inform NERC IA's plan for current and future audit activities and scope to help ensure effectiveness of CMEP activities. In addition, NERC IA will adapt its audit plan based on the periodic risk assessments.

[6] Standard 2500 – Monitoring Progress, in The Institute of Internal Auditors, *International Standards for the Professional Practice of Internal Auditing* (2016) at 20, https://www.theiia.org/globalassets/site/standards/mandatory-guidance/ippf/2017/ippf-standards-2017-english.pdf [hereinafter *IPPF Standards*].

As part of this follow up, NERC IA reports quarterly on the status of completion and effectiveness of MAPs to the NERC Compliance and Certification Committee ("CCC") and the NERC Board of Trustees Enterprise-Wide Risk Committee. In addition, as part of oversight, NERC and Regional Entity CMEP management track the progress of MAP completion and work with CMEP staff to help ensure consistent implementation of the CMEP in meeting the MAP milestones. While detailed MAP tasks are included in **Attachments A-G**, Subsections A and B below describe at a high level the MAPs that correspond with the observations in Section III of this filing. Subsection C provides the status of completion for Regional Entity MAPs.

A. Regional Entities

While each Regional Entity has specific MAPs, the majority of Regional Entity MAPs fell into the "Risk Assessment"[7] and "Compliance Oversight Plans"[8] categories. For example, all Regional Entities have a MAP related to Compliance Oversight Plan completion or process enhancement. NERC IA also assigns a risk level to observations (i.e., high, medium, or low) to assist in prioritization. In determining the risk level, NERC IA considers a variety of factors including, but not limited to, the potential impact of the risk and control issue, the likelihood of the potential impact occurring based on process or control gaps, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls. Most of the observations serving as the basis for Regional Entity MAPs fell into the medium risk category, with some low risk items and no high risk items.

Since the close of the audit period and development of recommendations, the Regional Entities have made good progress in implementing MAPs based on the audit recommendations.

[7] NERC IA included IRAs, regional risk assessment, Potential Noncompliance, and mitigating activities in the scope of the Risk Assessment category.

[8] Regional Entities develop a Compliance Oversight Plan to capture how a Regional Entity will monitor a registered entity's compliance with selected NERC Reliability Standards based on entity-specific risks.

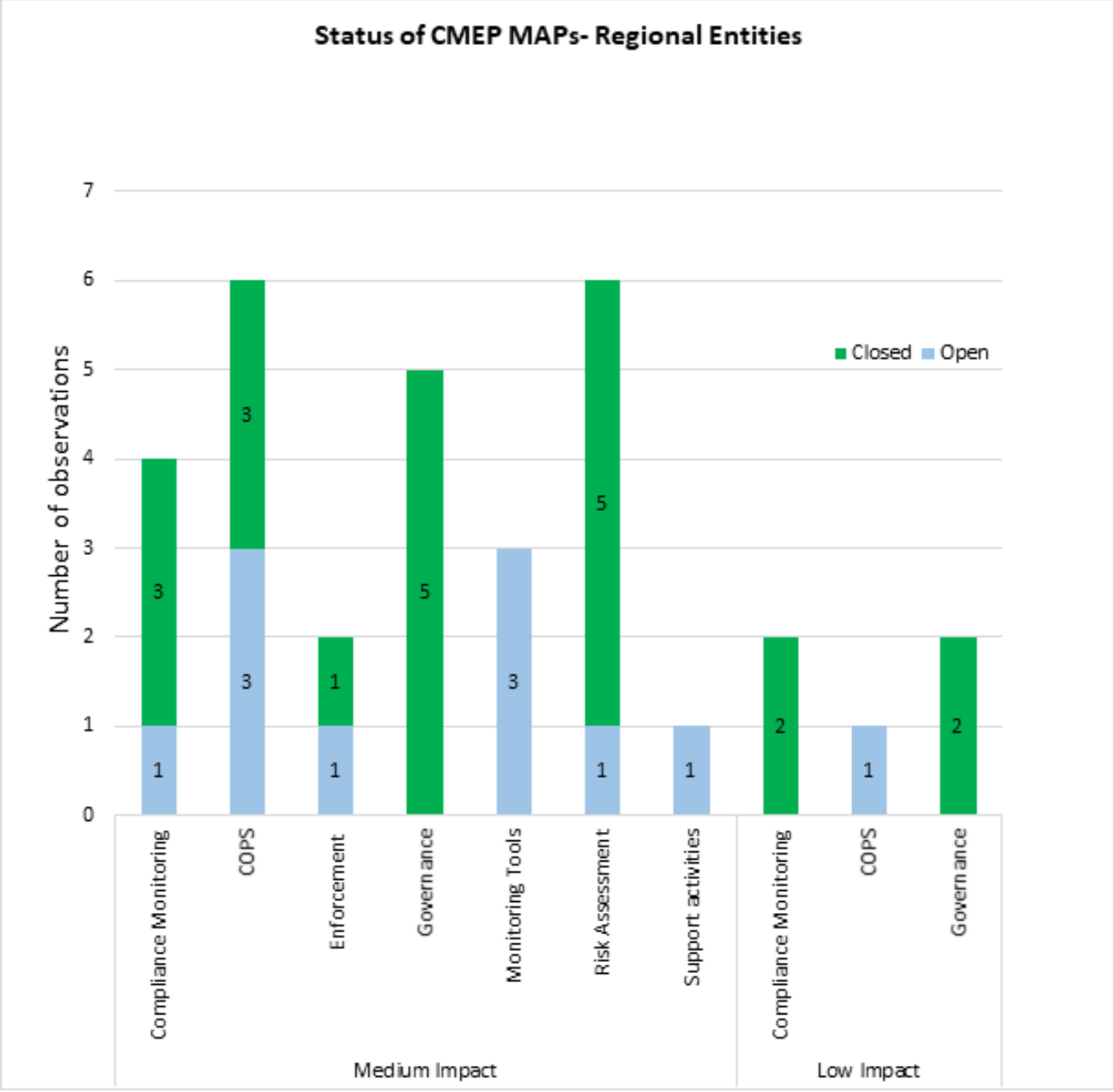
As of its last report to the NERC Board of Trustees in May, NERC IA reported that the Regional Entities completed 21 out of 32 total recommendations, which is nearly 66% of assigned MAPs. As of the time of this filing, NERC IA expects more recommendations to be completed by June 30, 2023. Tables 1 and 2 below demonstrate the progress as reported to the NERC Board of Trustees at its May quarterly meeting.[9] Table 1 indicates the number of recommendations open by each Regional Entity. Table 2 indicates the status of MAPs by topic area and risk level.

Table 1

Audit Engagement	Total Recommendations	Total Closed Recs.	Total Open Recs.	Repeat Recs.
2022 RE CMEP 4A Audit	32	21	11	0
MRO	6	2	4	0
NPCC	11	5	6	0
RF	3	3	0	0
SERC	5	4	1	0
Texas RE	3	3	0	0
WECC	4	4	0	0

[9] Regional Entities continue to make progress on MAPs and update NERC IA at regular intervals based on the committed deadlines.

Table 2



B. NERC

While NERC oversight of the CMEP was not directly in scope of the Appendix 4A audits, NERC IA identified areas where NERC oversight could assist in supporting Regional Entity implementation of the CMEP, resulting in recommendations for NERC. In response, NERC management developed MAPs for NERC staff, as described in **Attachment A** to this filing.

Moreover, NERC IA also completed its ROP Section 406 audit of the NERC CMEP in 2022, so those MAPs complement the Regional Entity Appendix 4A MAPs. The following are some key NERC strategies to improve the overall consistency of CMEP processes in response to the observations in the Appendix 4A audit engagements and to assist in executing MAPs.

1. Enhancements to the Align tool foster greater consistency across CMEP processes and programs.

The ERO Enterprise is committed to CMEP effectiveness and has invested very substantial resources in the Align tool to improve automation, efficiency, harmonization, and consistency. The Align tool now provides a single, common technology platform for the ERO Enterprise CMEP. Over the course of 2021, the ERO Enterprise launched various Align releases, which included Self-Reports, Self-Logs, Mitigation, Technical Feasibility Exceptions, Periodic Data Submittals, Attestations, and Compliance monitoring functionality (e.g., Audit, Spot Checks, and Self-Certifications). Through the release of version 4.5 of Align in 2023, Regional Entities can now use baseline templates for Inherent Risk Assessment ("IRA") development and summarization and Compliance Oversight Plans. These templates improve Regional Entity alignment by implementing consistent formats for CMEP processes and tools. Align release 4.5 will also address differences in Regional Entities' refresh processes by incorporating set triggers for review in the tool. NERC Compliance Assurance will apprise the Board of Trustees Compliance Committee of its oversight efforts by using the Align tool to monitor IRA and Compliance Oversight Plan completion and report results to the NERC Board of Trustees Compliance Committee.

The Align tool will include an automated Reliability Standards compliance audit functionality, which will facilitate a consistent ERO Enterprise approach for audit scope and audit notification. The audit pilot program extended through the second quarter of 2023. NERC

Compliance Assurance will collaborate with Regional Entities to evaluate: (1) Regional Entity justification documentation of audit scope and Compliance Oversight Plan variations; and (2) Regional Entity approaches to on-site and offsite audits.

The Align tool, Learning Management system, or regional tools are used, or will be used, to capture required auditor training completion. NERC Compliance Assurance will continue to provide required Auditor training, as well as periodically perform oversight, to ensure Regional Entity audit staff training is adequately documented, tracked, and up-to-date.

2. NERC will work to enhance consistency in implementation of Self-Certifications, controls evaluations, Complaints processing, and enforcement activities, including Self-Logging.

NERC Compliance Assurance will evaluate: (1) Regional Entity implementation of Self-Certification principles, inclusive of review timelines and potential noncompliance creation; and (2) Regional Entity processes for identified potential noncompliance during Self-Certification engagements. NERC Compliance Assurance will work with ERO Enterprise staff, Regional Entity management, and an internal controls task force, and others as needed, to develop additional guidance and training on internal controls. Such training should address: (1) consistent internal controls identification, documentation, and assessment approach during CMEP activities; and (2) a holistic Regional Entity approach for applying and sharing internal control information. NERC Compliance Assurance plans to collect and assess Regional Entity Complaint and Investigation processes for: (1) consistency across the ERO Enterprise; (2) efficiency; (3) thoroughness; and (4) communication.

NERC Enforcement commenced a Self-Logging oversight activity in the second quarter of 2023, to evaluate, among other things, any potential improvements to the program considering the parameters of FERC orders.

III. OVERVIEW OF APPENDIX 4A AUDITS

NERC IA conducted its audit engagements of the Regional Entities throughout 2022. Consistent with the requirements of Appendix 4A, NERC IA provided notification of the audit engagement to Regional Entity leadership prior to initiation of audit planning and on-site fieldwork. As described more fully in this section, NERC IA applied professional auditing principles to conduct audits of the Regional Entities to assess not only compliance with the ROP, but also the effectiveness of Regional Entity CMEP implementation. Through assessing effectiveness, NERC IA reviewed the quality of each audited Regional Entity's performance in carrying out its CMEP responsibilities. There were limited findings of ROP noncompliance, and NERC IA determined that all Regional Entities demonstrated the capability to perform CMEP administration and activities. NERC IA also identified several best practices and opportunities for improvement. The following section describes the Appendix 4A audit engagements and is divided into the following subsections: Subsection A describes the composition of the audit team; Subsection B covers the audits' objective, scope, and period; Subsection C provides an overview of NERC IA's audit approach; and Subsection D details observations resulting from the audit engagements.

A. Audit Team

The NERC Board of Trustees designated the NERC IA function, under the leadership of the Director of Internal Audit, as the audit team lead for the audits. Consistent with its charter, the IA function works to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. NERC IA staff adhere to the International Professional Practices Framework ("IPPF") promulgated by the Institute of Internal Auditors.[10] The IPPF

[10] The IPPF is available at https://www.theiia.org/en/standards/international-professional-practices-framework/.

includes mandatory standards and guidance to establish an IA function within an organization and conduct audits with effectiveness through the requisite independence and objectivity. Specifically, the Attribute Standards within the *International Standards for the Professional Practice of Internal Auditing* [11] mandate independence of the internal audit function, [12] individual auditors' objectivity,[13] and organizational independence[14] that serve to uphold the integrity of the internal audit function and its auditors. As is leading practice for internal audit departments, NERC internal auditors are members of the Institute of Internal Auditors. Such membership imposes obligations to adhere to the IPPF, including the principles of independence and objectivity, in order to engage in the profession of internal auditing.

The Director of IA reports functionally[15] to the NERC Board of Trustee's FAC and has unrestricted access to and regular communication with the FAC chair. The Director of IA also must confirm to the FAC, at least annually, the organizational independence of IA's internal audit activities. In its role as audit team lead for the Appendix 4A audits, IA plans, executes, and oversees the audit process and coordinates and facilitates the audit process steps with the Applicable Governmental Authorities, the CCC, and the audited Regional Entity. The audits were executed under the leadership of NERC IA resources, supplemented through staff augmentation

---

[11] *IPPF Standards*, *supra*.

[12] Interpretation of Attribute Standard 1100 describes independence as "the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels."

[13] Interpretation of Attribute Standard 1100 describes objectivity as "an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels."

[14] Interpretation of Attribute Standard 1110 states that organizational independence is "effectively achieved when the chief audit executive reports functionally to the board."

[15] The Director of IA reports administratively to NERC's General Counsel, resulting in a dual-reporting relationship.

through partnership with a leading audit firm, and conducted with observers from the CCC and FERC.

B. Audit Objective, Scope, and Period

The audit objective was to assess the Regional Entities' implementation of the CMEP to determine whether they effectively meet the requirements under the ROP Section 400 *et seq.*; Appendix 4C; the corresponding annual CMEP IP, including monitoring and enforcement of compliance with relevant Reliability Standard requirements; and the delegation agreements. Consistent with ROP Section 402.1.3 and Appendix 4A, the scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements, and associated areas of focus and monitoring schedules. Specifically, the audit scope assessed activities within the following categories: (1) governance; (2) risk assessment, including IRAs; (3) Compliance Oversight Plans; (4) enforcement activities and actions; (5) compliance monitoring processes and tools; and (6) supporting activities, such as methodologies and processes. More detailed descriptions of the scope within each category for each Regional Entity are provided in **Attachments B-G** to this filing.

In addition, the audit engagement included an evaluation of each Regional Entity's approach to and application of the risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC.[16] NERC IA auditors did not limit the scope to only assessing compliance with applicable "shall statements" in governing documents. Rather, the scope of the audit engagements included the various components (e.g., IRA, Compliance Oversight Plans, self-logging, etc.) of the implementation of the CMEP to assess effectiveness of

[16] The audit scope did not specifically include NERC's oversight responsibilities over the Regional Entities' implementation of the CMEP. However, the observations and recommendations summarized in this filing recognize NERC staff collaboration with Regional Entities in implementing MAPs as part of the continued improvement of the CMEP.

each Regional Entity's implementation. To further inform the scope, NERC IA considered its annual risk assessment process, discussions with members of management and relevant stakeholders, and qualitative and quantitative factors. The resulting scope led to a comprehensive audit of each Regional Entity's CMEP implementation. The audit period covered January 1, 2020 through December 31, 2021, with NERC IA expanding evaluation when necessary based on program activity frequency or changes.[17]

C. Audit Approach

In achieving the objective of the audit engagement within the scope of program components under review, NERC IA employed several auditing techniques to gain assurance of the effectiveness of each Regional Entity's CMEP implementation. These techniques include inquiry, inspection, observation, re-performance, and analytical procedures. When employing these techniques, NERC IA used widely accepted audit sampling techniques to obtain audit evidence that is sufficient, appropriate, and necessary to arrive at a conclusion based on the sampling technique used.

Through the use of these selected auditing techniques, NERC IA assessed the quality of performance of each Regional Entity. This assessment included not only confirming past compliance with the ROP, delegation agreements, and other relevant authority during the audit period but also gaining assurance of the effectiveness of processes and controls for continually meeting these obligations going forward. To that end, the assessment included review of opportunities for continuous improvement even where compliance with the ROP has been maintained. As a result, NERC IA engaged in a comprehensive audit that sought to ensure

[17] Consistent with current risk-based auditing practices, NERC IA audits the most recent activities relevant to current program processes. In addition, the last set of targeted Appendix 4A audits for the prior Five-Year Assessment period was June 1, 2014 – December 31, 2018. The Appendix 4A audits commenced in January 2022.

consistency and fairness among Regional Entity CMEP implementation by looking beyond the compliance requirements over the audit period.

For each Regional Entity, NERC IA evaluated its application of monitoring tools such as periodic risk assessments and analyses, IRAs, Compliance Oversight Plans, Compliance Audits, Self-Certifications, Spot Checks, Self-Logging, and Periodic Data Submittals to establish compliance monitoring intervals. Furthermore, core CMEP governance activities included a review of the depth and breadth of training and learning programs administered across the CMEP, including Regional Entity focus on the importance of creating understanding of, and demonstrating proficiency with, internal controls as a critical component to risk-based oversight. Additional governance activities included: an understanding of complaint and investigation processes, review of complaints received and investigations performed during the period of the audit, and oversight performed to ensure independence over CMEP activities related to Regional Entities operating with hybrid boards.

D. Observations

Overall, NERC IA concluded that the Regional Entities have demonstrated the capability to administer the CMEP. NERC IA did not detect significant noncompliance with the ROP. Moreover, many Regional Entities have developed innovative practices regarding CMEP oversight of registered entities in their planning, scheduling, and execution of monitoring activities. Nevertheless, Regional Entity variability persists in the implementation of the CMEP that leads to inconsistent CMEP practices and outcomes for registered entities. This variability exists in elements of some of the Regional Entities' CMEP oversight strategy, application of tools, and use of approved templates. Furthermore, Regional Entities differ in how they identify and mitigate risks, which impacts the scope, frequency, and execution of monitoring activities.

Additionally, tools needed to execute a risk-based oversight strategy, such as IRAs and Compliance Oversight Plans, are not always developed and refreshed consistently across Regional Entities. While specific observations for each Regional Entity are located in **Attachments B-G** of this filing, below is a summary of the aggregated observations after completing all Regional Entity audit engagements. Because these are aggregated observations, not all of the below observations apply to each Regional Entity.

1. Approaches differed as to IRA and Compliance Oversight Plan implementation, particularly in developing and refreshing IRAs and Compliance Oversight Plans.

NERC IA observed some best practices during the audit fieldwork as well as some opportunities for improvement, particularly in implementing IRAs, Compliance Oversight Plans, and Self-Logging. Risk assessment and planning monitoring activities based on that risk are primary drivers of the risk-based compliance monitoring strategy for each registered entity. As such, NERC IA selected IRAs and Compliance Oversight Plans for evaluation due to their impact on the success of risk-based CMEP implementation. As described in more detail below and in **Attachments B-G**, all Regional Entity audit reports include observations related to IRAs or Compliance Oversight Plans.

An IRA is a review by a Compliance Enforcement Authority ("CEA") of potential risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as, but not limited to, assets, system, geography, interconnectivity, prior compliance history, and factors unique to the registered entity. The results of an entity-specific IRA are one input into the scope and type of compliance monitoring for a particular registered entity. Due to the wide scope of operational responsibility assigned to entities registered as Balancing Authorities ("BAs"), Reliability Coordinators ("RCs"), and Transmission Operators ("TOPs") as well as the ROP requirement that they undergo a compliance audit once every three years, NERC IA observed

that IRAs are prioritized for BAs, RCs, and TOPs. Other entities performing different registered functions may be ranked as having a lower inherent risk to the BPS. Thus, NERC IA observed that Regional Entities granted lower priority to these IRAs.

NERC IA also observed that the development of IRAs and the frequency for refreshing IRAs was at times inconsistent across the Regional Entities. In terms of development, NERC IA documented that some Regional Entities did not have initial IRAs developed for certain low risk registered entities until more than 2 years after their registration. While inherent risk can remain relatively static for registered entities in some respects once an IRA is developed, NERC IA recommends that Regional Entities without consistent triggers for refreshing IRAs implement them to help ensure factors that can impact inherent risk are incorporated into IRAs in a timely manner.

For IRA refreshment, the process for re-evaluating an IRA varied across regions. Factors considered included: (1) whether an entity was a RC, TOP, or BA and thus subject to a three-year audit requirement; (2) the results of an annual or semi-annual risk assessment or questionnaire sent to registered entities; (3) changes in registration; and (4) performance considerations from planned monitoring activity. In addition, evidence of management review or approval of refreshed IRAs was also at times inconsistent. Finally, some of the Regional Entities lacked consistency in their IRA templates and in maintaining evidence that management review or approval occurred.

The Regional Entities use Compliance Oversight Plans to further tailor the compliance monitoring oversight strategy for each registered entity, factoring in the registered entity's IRA as well as the CMEP IP and other registered entity performance considerations, such as compliance history, events, and internal controls. When compared across registered entities, Compliance Oversight Plans are also used to inform Regional Entity CMEP staff resource allocation and

oversight planning for the Regional Entity footprint. Regional Entities have been completing Compliance Oversight Plans for registered entities.

For the audit period, NERC IA found that the Regional Entities completed Compliance Oversight Plans for approximately 55% of registered entities on the NERC Compliance Registry. Similar to IRA refreshment, Regional Entities refresh Compliance Oversight Plans to ensure that their compliance monitoring of registered entities reflects the most up-to-date strategy for registered entities based on their current risk and compliance posture. Similar to IRAs, NERC IA observed that there is variation among some of the Regional Entities regarding: (1) the criteria that trigger the need to refresh a Compliance Oversight Plan, (2) the processes used to conduct the Compliance Oversight Plan refresh, and (3) the existence of evidence to demonstrate that the Compliance Oversight Plan review had occurred.

2. NERC IA observed compliance audit planning and notification opportunities for improvement and differences in on-site versus offsite audit approach.

Under the ROP, Compliance Audits are the most in-depth compliance monitoring process and involve the most interaction with registered entities. As such, NERC IA selected compliance audits for the Appendix 4A audit scope to assess consistency and fairness across these high-interaction compliance monitoring processes. The scope of a compliance audit for a registered entity should be tailored to include Reliability Standards identified through the NERC-approved risk-based processes, including internal controls, IRAs, and other inputs. As a result, the CEA is not bound by the Reliability Standards requirements identified in the ERO CMEP Implementation Plan during this scoping exercise.

NERC IA found that compliance audit scoping has several areas for improvement. First, NERC IA found that for some Regional Entities, some Audit Notification Letters to registered entities did not effectively communicate the scope of audits. For example, some Audit Notification

Letters included Reliability Standards requirements in scope that were not part of the registered entity's Compliance Oversight Plan. While an audit scope can include requirements not identified in the Compliance Oversight Plan due to risk-based considerations, Regional Entities should communicate those considerations to registered entities to explain the risk-based reasoning behind the differences in the audit scope and the Compliance Oversight Plan. Second, Regional Entities varied in how they used Compliance Oversight Plans to scope registered entity audits.

NERC IA identified an opportunity for Regional Entities to further align processes regarding how they select and how they implement the suite of monitoring tools outlined in Appendix 4C to the ROP. For instance, Spot Checks and Periodic Data Submittals are not widely utilized at some of the Regional Entities. As another example, one Regional Entity used different auditing techniques for on-site versus offsite audits. The Regional Entity used interviews for on-site audits but minimized use of interviews for offsite audits.

3. Regional Entities implement the use of self-certifications differently.

A CEA may require registered entities to self-certify their compliance with Reliability Standards. In the ROP, a Self-Certification is defined as an "attestation" that a registered entity is compliant or non-compliant, which typically means an entity may not need to produce evidence. However, half of the Regional Entities implement this oversight tool as a "guided Self-Certification," which requires registered entities to submit compliance evidence along with the attestation. As such, a "guided Self-Certification" shares many characteristics of a limited scope audit. Furthermore, in some cases, all such evidence is reviewed by Regional Entity staff similar to a Compliance Audit. Some Regional Entities focus this process only on Critical Infrastructure Protection Reliability Standards while others also include operations & planning Reliability Standards. While a Self-Certification is not construed as a finding that the registered entity is or is not compliant with, or subject to or not subject to, a Reliability Standard, NERC IA found that the

Regional Entities should align on a process or guidance for recording any *potential* noncompliance identified during the process to maximize efficiency and consistency.

4. Regional Entities differ in understanding and evaluation of registered entities' internal controls.

Internal controls are fundamental to a risk-based approach to ensuring reliability. Internal controls minimize overall risk for failure of compliance. As such, an evaluation of internal controls is an important input into both risk-based compliance monitoring planning (e.g., how deeply an auditor must look into evidence for reasonable assurance of compliance) and gaining assurance that a registered entity can maintain an effective program going forward. Given the role internal controls play in a risk-based framework, NERC IA selected internal controls as an area of focus for the audit engagements.

NERC IA identified opportunities for some Regional Entities to improve their understanding and awareness of internal controls as well as techniques to evaluate such internal controls. For example, staff at one Regional Entity requested that a registered entity develop an internal controls program but did not engage in follow up discussions on what that program should look like or whether the program was developed and implemented appropriately. NERC IA recommended that Regional Entities use training, guidance, and learning programs if not already in use to educate Risk Assessment and Mitigation personnel and CMEP personnel about how internal controls operate within a risk-based oversight model. Such programs should be framed consistent with industry leading governance, risk, and control frameworks and standards.

5. In enforcement activities, some Regional Entities have inconsistent handling of potential noncompliance triage, Open Enforcement Actions, and Self-Logging.

Not all instances of noncompliance with Reliability Standards require the same type of processing and documentation. Noncompliance that does not pose a serious or substantial risk to

the reliability of the BPS may be resolved through streamlined processes, when appropriate. These streamlined processes include the Find, Fix, Track, and Report ("FFT"); and Compliance Exception processes. A Regional Entity has discretion to pursue these alternatives after a Preliminary Screen is completed and the Regional Entity identifies a potential noncompliance. NERC IA did recommend that some Regional Entities better document "triage" processes to help direct potential Reliability Standards noncompliance to these alternative resolution processes, as applicable. As a result, in some instances there are backlogs for instances of potential noncompliance captured in off-line format as minimal risk but not entered into Align with timely reporting and disposition. Some of the Regional Entities also differ in their use of monitoring activities and tools when there are open enforcement actions that have not been mitigated.

Participation in the Self-Logging program is on average at 8% of all registered entities within the ERO Enterprise. NERC IA found that promotion of the program and its benefits varies across the Regional Entities. Half of Regional Entities do not differentiate between Self-Logging and Self-Reporting, minimizing the benefit of the program. NERC IA also found that program application processes are inconsistent across some of the Regional Entities in terms of requirements and qualifications for eligibility for the Self-Logging program.

6. Handling of complaints was inconsistent across some of the Regional Entities.

Regional Entities may receive Complaints alleging violations of a Reliability Standard. Compliance Investigations, or other compliance monitoring processes, may be initiated at any time by a Regional Entity in response to such a Complaint, or in response to a system disturbance, or any other potential noncompliance with a Reliability Standard identified by any other means. In a two-year period, approximately 6 Complaints were logged and 3 Compliance Investigations were conducted across all Regional Entities. Handling, communication, and resolution of anonymous

complaints was inconsistent between Regional Entities and NERC. NERC IA also found that disposition of complaints was premature in some cases and did not adequately address reported internal control issues that may contribute to violation of Reliability Standards.

7. Regional Entities lacked a process to track completion of required training and learning.

As part of its oversight, NERC CMEP staff coordinates and delivers learning materials, resources, and activities to train and educate ERO Enterprise staff supporting statutory and delegation-related activities. NERC IA found that there is no process to designate and track required training of auditors or lead auditors. NERC IA also identified a need to enhance lead auditor training. This will help to verify that required training occurred prior to audit engagements or on a stated frequency.

8. NERC IA highlighted several best practices across Regional Entities that can inform improvements to overall implementation of the CMEP.

NERC IA identified several best practices across the Regional Entities that can be widely adopted to improve the implementation of the CMEP and related processes. These best practices were attributed to the Regional Entities' strong leadership and focus on the most optimal structure, subject matter expertise, and innovations necessary to administer an effective CMEP. Best practices include locally designed, developed, and implemented automated tools to represent registered entities within the Regional Entity footprint. These tools helped to more effectively evaluate risk, plan, and schedule monitoring activity as well as analyze or retain performance data relevant to determining the appropriate oversight strategy, monitoring activities, tools, and associated monitoring intervals. In addition, the majority of the Regional Entities implemented Entity Risk Profile tools and processes to capture inherent risk changes and incorporate and refresh performance data and results of monitoring activity to inform annual planning.

IV. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission accept this compliance filing as meeting NERC ROP Section 402.1.3 and the directive in the Order on Compliance Filings.

Respectfully submitted,

/s/ Marisa Hecht

Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: June 30, 2023

CERTIFICATE OF SERVICE

I hereby certify 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 Washington, D.C., this 30th day of June 2023.

/s/ Marisa Hecht

Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street, N.W., Suite 410
Washington, D.C. 20005
(202) 400-3000
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment A

Appendix 4A Audit Report – Consolidated Executive Summary

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL EXECUTIVE SUMMARY

CMEP Regional Entity Audit (Appendix 4A)

Consolidated Executive Summary

October 13, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Sonia Mendonca, Senior Vice-President and General Counsel
Jim Robb, President and CEO

From: NERC Internal Audit

Date: October 13, 2022

Subject: Regional Entity Compliance Monitoring and Enforcement Program Audit

****

Enclosed is a consolidated Executive Summary of Internal Audit's observations related to Compliance Monitoring and Enforcement Program (CMEP) 4A Audits performed at the six Regional Entities.

The audit objective was to assess the Regional Entities' implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements placed in the CMEP IP.

This Executive Summary provides additional context and summarizes broad themes from the observations described in greater detail in the individual audit reports already issued to each Regional Entity. It is intended to aid NERC, working within the ERO Enterprise collaboration structure, in pursuing enhancements to the implementation of the CMEP and notes actions that NERC CMEP management has agreed to undertake in connection with the observations. It is not intended to modify the management action plans (MAPs) adopted in the individual Regional Entity audit reports.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Jim Albright (TexasRE)
Jason Blake (SERC)
Manny Cancel
Charles Dickerson (NPCC)
Melanie Frye (WECC)
Tim Gallagher (ReliabilityFirst)
Kelly Hanson
Mark Lauby
Sara Patrick (MRO)
Janet Sena
Mechelle Thomas

EXECUTIVE SUMMARY

CMEP Appendix 4A Audit – Consolidated Observations and Recommendations

Background

NERC, as the Electric Reliability Organization (ERO), established the Compliance Monitoring and Enforcement Program (CMEP) to facilitate the "ongoing monitoring of user, owner and operator compliance with Reliability Standards." The North American Bulk Power System (BPS) is monitored by the following six Regional Entities with corresponding boundaries: Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst, SERC Reliability Corporation, Texas Reliability Entity, and Western Electricity Coordinating Council. Included in the Appendix is an illustrative view of each Regional Entity footprint and CMEP staff for comparison at the time of audit.

In February 2015, the ERO Enterprise adopted a risk-based approach to the implementation of the CMEP in accordance with the Reliability Assurance Initiative (RAI), approved by Federal Energy Regulatory Commission (FERC). Significant components of the risk-based CMEP entailed developing Inherent Risk Assessments (IRAs), focusing efforts and reliance on evaluating the effectiveness of an entity's internal controls, deploying the compliance exception process to record and mitigate risks without formal enforcement action, and implementing a self-logging program for eligible registered entities to consolidate self-reporting of minimal risk noncompliance to be processed as compliance exceptions. This approach improved processing time of minimal to moderate risk noncompliance and broadened NERC and Regional Entity use of entity-specific risk assessments to determine audit scope and frequency. Over the past few years, NERC and the Regional Entities have implemented CMEP improvements, such as a single CMEP information system, Align, and enhancements to tools integral to effective monitoring, such as Compliance Oversight Plans (COPs), to establish a transparent CMEP oversight strategy for a registered entity with assigned monitoring tools and intervals based on a comprehensive assessment of risk.

NERC oversees each Regional Entity that has been delegated authority to, among other things, implement an effective CMEP. The objective of this oversight is to ensure that the Regional Entity carries out its obligations under the CMEP effectively, and in accordance with the Rules of Procedure (ROP) and the terms of the Regional Delegation Agreement (RDA), and to ensure consistency and fairness of the Regional Entity's execution of the CMEP.

In accordance with ROP Section 402.3.1 and Appendix 4A, the NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC CMEP and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC ROP, and the corresponding annual CMEP Implementation Plan (IP).

As a result of a directive in the FERC Order on the Five-Year Performance Assessment issued on January 19, 2021, NERC Internal Audit independently planned and performed audits of each Regional Entity's implementation of the CMEP. The audits were executed under the leadership of NERC Internal Audit resources, supplemented through staff augmentation through partnership with a leading audit firm, and conducted with observers from FERC and the Compliance and Certification Committee (CCC). The audit findings and recommendations have been shared with NERC and the six Regional Entities, and management action plans have been developed to address process, control, and compliance observations. Further, we look forward to completing our independent audit of the NERC CMEP in accordance with Section 406 of the ROP, which will further inform our overall observations and conclusions to collectively improve the CMEP.

Audit Summary

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus, and an evaluation of the Regional Entity's approach to and application of the risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC. The audit scope did not specifically include NERC's oversight responsibilities over the Regional Entities' implementation of the CMEP. However, we acknowledge these responsibilities and understand that NERC staff leading CMEP functions intend to work collaboratively with the Regional Entities to address the observations summarized below as part of the continued improvement of the CMEP.

Our observations did not detect significant noncompliance with the ROP. Specific deviations were identified, communicated within the respective Regional Entity audit reports, and should not be implied in other observations and conclusions. Furthermore, our conclusions underscore a need to enhance NERC oversight activities to continue to drive greater adoption of the risk-based methodology, further harmonization of processes, and more effective use of monitoring tools across the ERO Enterprise.

We concluded that all Regional Entities demonstrated the capability and access to data, tools, guidance and templates to perform CMEP administration and activities, which include the consistency and harmonization of processes and tools enabled by the ERO Enterprise implementation of Align. In addition, while local innovations and enhancements provide a more integrated approach to CMEP oversight, planning, scheduling, and execution of monitoring activities, the Regional Entities and NERC should consider a common path to use the full functionality of Align and standard processes, tools and templates to support more consistency in the implementation of the CMEP. This common path will drive consistency of the CMEP risk-based oversight strategy by identifying, assessing and mitigating risks guided by common processes and use of standard tools and templates that ensure reliability and security.

During the course of our evaluation, we identified several best practices across the Regional Entities, as well as opportunities to improve the implementation of the CMEP and related processes. These best practices were attributed to the Regional Entities' strong leadership and focus on the most optimal structure, subject matter expertise and innovations necessary to administer an effective CMEP. Best practices consisted of locally designed, developed and implemented automated tools to represent registered entities within the Regional Entity footprint, to more effectively evaluate risk, plan and schedule monitoring activity, and analyze, or retain performance data relevant to determining the appropriate oversight strategy, monitoring activities, tools and associated monitoring intervals. In addition, the majority of the Regional Entities implemented Entity Risk Profile ("ERP") tools and processes as a mechanism to capture inherent risks changes, and incorporate and refresh performance data and results of monitoring activity to inform annual planning.

Our audit approach and procedures included a comprehensive evaluation of each Regional Entity's application of a risk-based oversight strategy and use of monitoring tools such as periodic risk assessments and analyses, IRAs, COPs, Compliance Audits, Self-Certifications, Spot Checks, Self-Logging and Periodic Data Submittals (PDS) to establish compliance monitoring intervals. Furthermore, core CMEP governance activities included a review of the depth and breadth of training and learning programs administered across the CMEP, including Regional Entity focus on the importance of creating understanding of, and demonstrating proficiency with internal controls as a critical component to risk-based oversight. Additional governance activities included: an understanding of complaint and investigation processes, review of complaints received and investigations performed during the period of the audit, and oversight performed to ensure independence over CMEP activities related to Regional Entities operating with hybrid boards.

A significant area of opportunity in the evolution of the ERO Enterprise's risk-based approach is to move the oversight approach to a holistic framework, inclusive of an ongoing assessment of all registered entities (e.g.,

accounting for all assets within their respective footprint and impact to the BPS) beyond functions subject to a three year audit requirement and to achieve greater balance in the use of use of monitoring tools with sufficient rationale for monitoring intervals to ensure the effectiveness of the CMEP in promoting reliability and security.

Elements of the CMEP oversight strategy, application of tools, and use of approved templates vary from Regional Entity to Regional Entity. Also, the application of a risk based approach is defined differently by each Regional Entity as illustrated with variation in scope, frequency, and execution of monitoring activities, such as Compliance Audits, performance of Self-Certifications focused on Critical Infrastructure Protection (CIP) or Operations and Planning (O&P) Reliability Standards, and half of Regional Entities' applying a concept of a "guided self-certification" which equates to a limited scope audit. Additionally, tools integral to the execution of a risk-based oversight strategy and the establishment of monitoring tools and intervals, such as IRAs and COPs, were developed and refreshed inconsistently across Regional Entities.

To illustrate aspects of the variations in risk-based oversight strategy, and use of program tools and templates, several visual representations are included in Appendix A on page 10, within the Consolidated Executive Summary. These are provided to aid NERC and the Regional Entities in working towards further consistency and are not intended as separate or additional observations or findings.

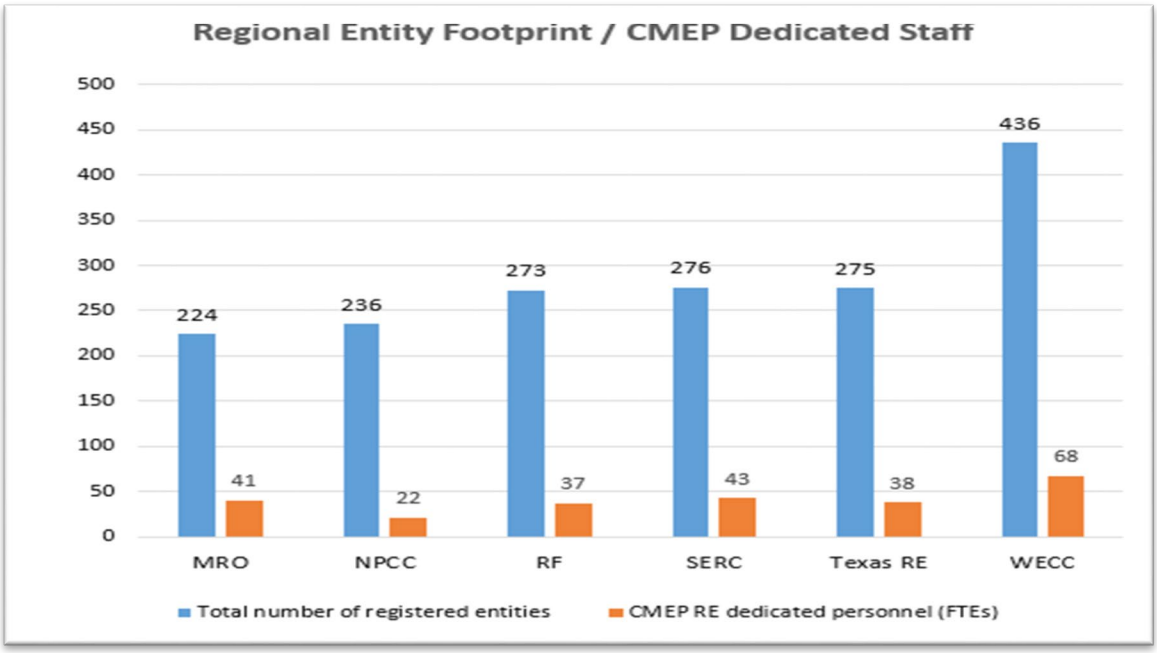
Aggregated Observations (Inclusive of the six Regional Entities)	
Observation	**Management Action Plan (MAP) Summary**
IRAs • Risk-based approach to developing and refreshing IRAs is primarily influenced by registered entities with BA/RC/TOP functions and the associated ROP requirement for a Compliance Audit at least once every three years • Registered entities ranked as low risk entities generally did not have an IRA developed until 2+ years after registration • Frequency for refreshing IRAs was inconsistent across the Regional Entities; some based on annual or semi-annual risk assessments/questionnaires, changes in registration, and performance considerations from planned monitoring activity • Templates varied across Regional Entities, including the performance risk analyses and risk summaries • Evidence of management review/approval was inconsistent	NERC Compliance Assurance will collaborate with Regional Entities to collect the Regional risk-based IRA development and refresh processes • As appropriate, NERC Compliance Assurance will work with the Regional Entities to develop a consistent approach across ERO Enterprise Align release 4.5, currently scheduled for November 2022, will address future template concerns as Align will be the tool for IRA development and summarization. NERC Compliance Assurance will monitor: • IRA completion and report results to the BOTCC; and • Registered entity IRA refresh processes and gauge current to expected progress
COPs • Approximately 55% of registered entities have a COP • Refresh frequency varied across Regional Entities; refreshes occurred before a Compliance Audit, or after, and in some cases were not refreshed until two years after an audit • Templates and development processes vary across the Regional Entities without specific guidelines for when to complete or refresh a registered entity's COP • Evidence of management review/approval was inconsistent	NERC Compliance Assurance will collaborate with Regional Entities to collect the Regional risk-based COP development and refresh processes • As appropriate, NERC Compliance Assurance will work with the Regional Entities to develop consistent approach across ERO Enterprise Align release 4.5, currently scheduled for November 2022, will address future template and approval process concerns as Align will be the tool for COP development NERC Compliance Assurance will monitor: • COP completion and report results to the BOTCC; and • Registered entity COP refresh processes and gauge current to expected progress

Compliance Audits • Audit Notification Letters did not effectively communicate scope and varied in comparison to COPs • Differentiation between on-site and off-site audit approaches varied across the Regional Entities	Align audit functionality automates a consistent ERO Enterprise approach for audit scope and audit notification. The audit pilot program is extended through 2Q 2023. NERC Compliance Assurance will collaborate with Regional Entities to evaluate: • Regional Entity justification documentation of audit scope and COP variations; and • Regional Entity approaches to on-site and off-site audits NERC Compliance Assurance will continue to monitor: • ROP audit scope and notification requirements; and Regional Entity audit approaches for on-site and off-site audits
Self-Certifications • 50% of REs apply a concept of "guided self-certifications", which share many characteristics of a limited scope audit; evidence of compliance is required and in some cases 100% reviewed by Regional Entity staff • Scope of Self-Certifications vary across Regional Entities; some focus only on CIP, while some include both CIP and O&P • Process or guidance for recording Potential Noncompliance (PNC) identified during Self-Certifications is not defined, resulting in significant delays in recording and reporting PNCs in a few cases	NERC Compliance Assurance will collaborate with Regional Entities to evaluate: • Regional Entity implementation of self-certification principles (Review timelines and PNC creation); and • Regional Entity processes for identified possible noncompliance during self-certification engagements NERC Compliance Assurance will monitor potential noncompliance submitted through the self-certification process to ensure timely submittal
Internal Controls • Understanding and awareness of internal controls is inconsistent across Risk Assessment and Mitigation (RAM) and Compliance Monitoring and Enforcement personnel, including compliance auditors and techniques to evaluate during audit engagements • Evaluation of internal controls within monitoring activities or programs is inconsistent; compliance audits, self-logging, self-certifications and COPs • Absence of specific training, guidance and learning programs that reinforce the importance of internal controls within a risk-based oversight model consistent with industry leading governance, risk and control (GRC) frameworks and standards	NERC Compliance Assurance will continue to work with ERO Enterprise staff, the RPMG and its Internal Controls Task Force, and others as needed, to develop additional guidance and/or training on internal controls, including: • Consistent internal controls identification, documentation, and assessment approach by Regional Entities during CMEP activities; and • Holistic Regional Entity approach for applying and sharing internal control information. NERC Compliance Assurance will periodically monitor Regional Entities implementation of developed internal control guidance/training.

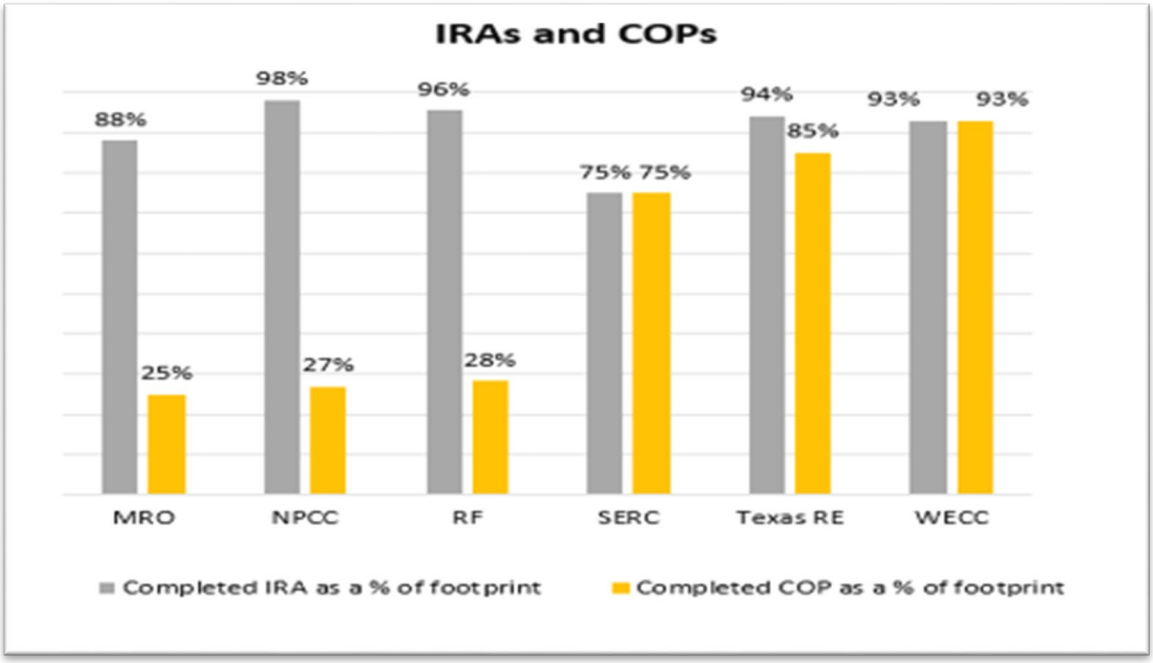
Enforcement Processes • Undocumented and inconsistent "triage" processes for PNC handling; backlogs occurred with PNCs captured in off-line format as minimal risk and not entered into system with timely reporting and disposition according to ROP • Monitoring activities and tools varied across Regional Entities related to handling of Open Enforcement Actions	NERC Enforcement will continue ongoing activities with the ERO Enterprise Enforcement Group (EG) to explore best practices for eliminating backlogs. NERC Enforcement is already seeing Regions adopting the best practices of other Regions NERC Enforcement will work with the EG to consider developing meaningful metrics for processing enforcement matters NERC Enforcement will also continue quarterly meetings with each Regional Entity to discuss caseloads and strategies for resolving older cases
Self-Logging • Participation in the program is on average at a nominal 8% of all registered entities within the ERO Enterprise • Promotion of the program and benefits is not understood or endorsed by the Regional Entities; 50% of Regional Entities do not differentiate between self-logging and self-reporting, minimizing the benefit of the program • Program application processes are inconsistent across the Regional Entities in terms of requirements and qualifications for eligibility according to ROP	NERC Enforcement will work with the EG to reevaluate the program in light of recent FERC orders NERC Enforcement will conduct a Self-Logging oversight activity in 2023, to evaluate, among other things, any potential improvements to the program considering the confines of FERC orders
Complaints and Investigations • In a two-year period, approximately 6 complaints were logged and 3 investigations across all Regional Entities • Handling, communication and resolution of anonymous complaints was inconsistent between Regional Entities and NERC • Disposition of complaints was premature in some cases and did not adequately address reported internal control issues that may contribute to violation of Reliability Standards	NERC Compliance Assurance will collaborate with Regional Entities to collect and assess Regional Entity Complaint and Investigation processes for: • Consistency across the ERO Enterprise; • Efficiency; • Thoroughness; and • Communication process
Training and Learning Programs • A process to designate and track required training of auditors and lead auditors was not in place, making it difficult to verify that required training occurred prior to audit engagements and/or on a stated frequency • Evidence of more comprehensive lead auditor training was lacking	The Align tool, Learning Management system, or regional tools are, or will be used, to capture required auditor training completion NERC Compliance Assurance will continue to provide required Auditor training, as well as periodically perform oversight to ensure regional audit staff training are adequately documented, tracked, and current

Appendix A – CMEP Data Visualizations (Illustrative)

CMEP Registered Entity Footprint by Regional Entity in comparison to CMEP Staff

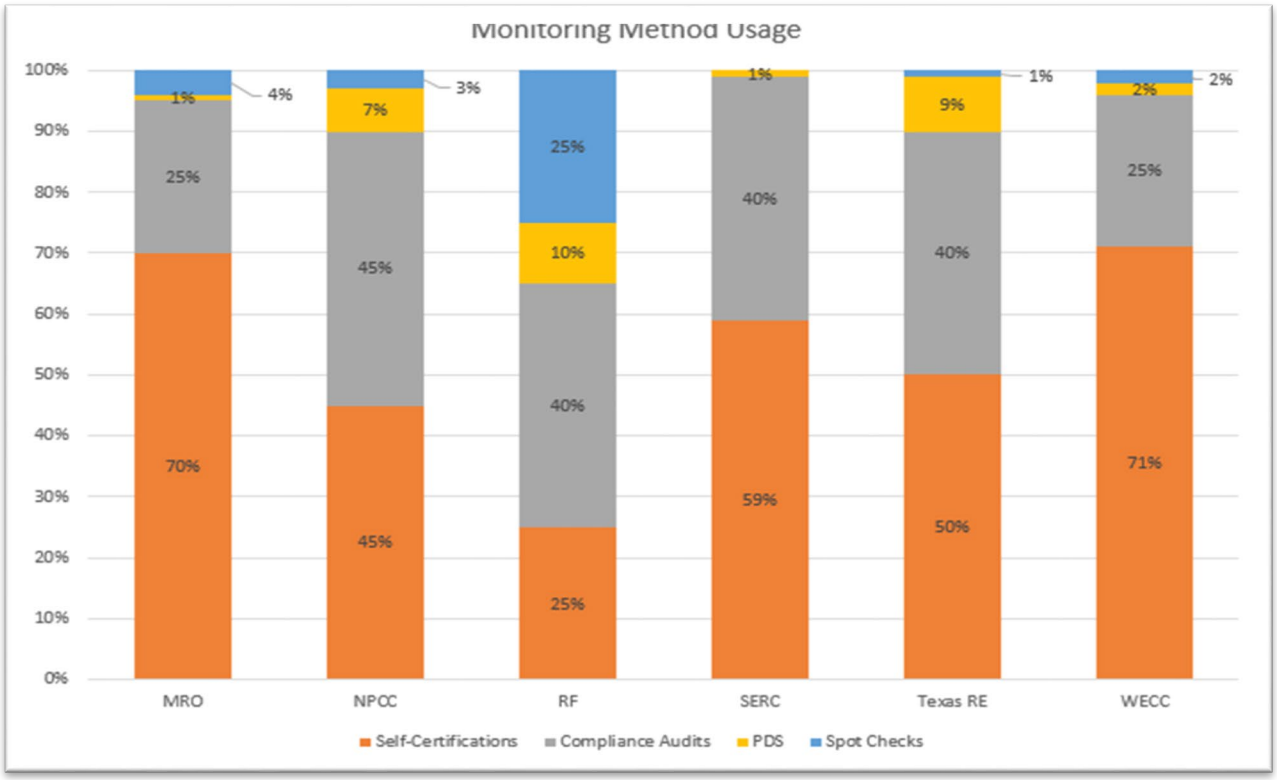


CMEP IRA and COP development as a percentage of total registered entities in Regional Entity footprint

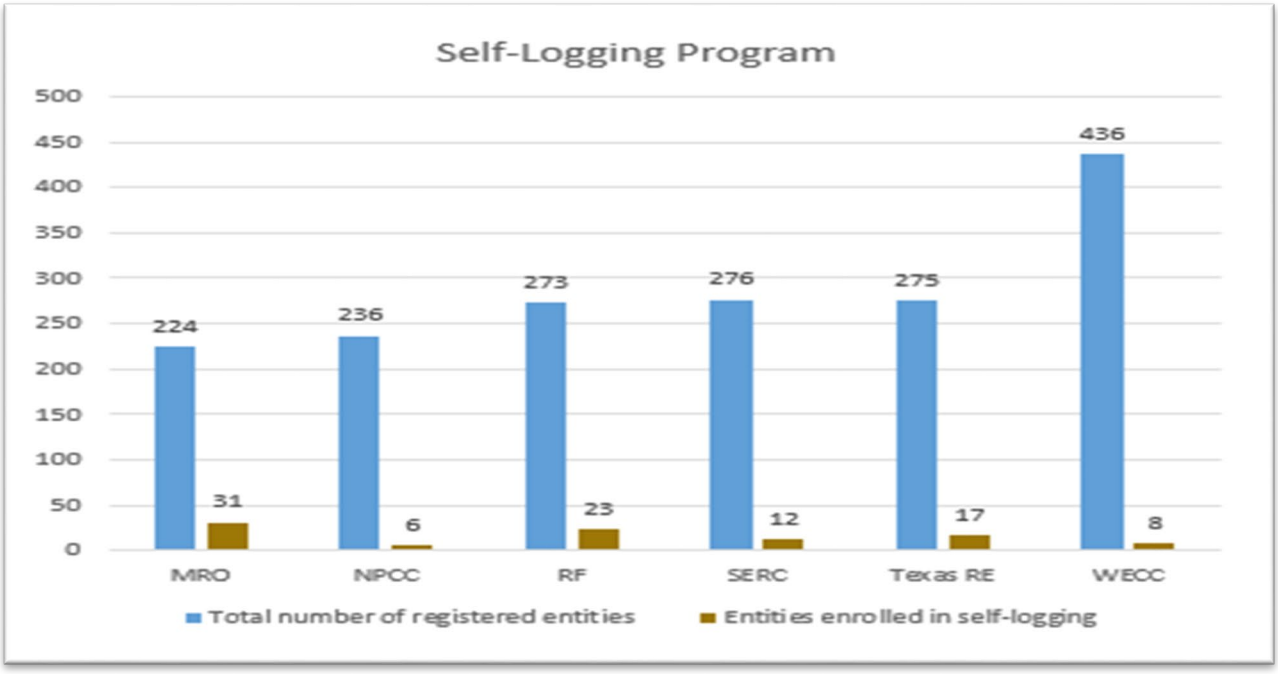


Appendix A – CMEP Data Visualizations (Illustrative) – con't

CMEP - Tool Usage



Self-Logging Program Enrollment



Appendix B

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, ROP requirements, and discussions with members of management and relevant stakeholders, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the governing NERC Board Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment B

Appendix 4A Audit Report – Midwest Reliability Organization

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

Midwest Reliability Organization (MRO)

Date: May 23, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Sara Patrick, President and Chief Executive Officer
Richard Burt, Senior Vice-President and Chief Operating Officer

From: NERC Internal Audit

Date: May 23, 2022

Subject: Regional Entity CMEP 4A Audit – Midwest Reliability Organization (MRO)

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity (RE) Compliance Monitoring and Enforcement Program (CMEP Appendix 4A) Audit.

The audit objective is to assess the RE's implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, Appendix 4C, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreements.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Manny Cancel (NERC)
Kelly Hanson (NERC)
Mark Lauby (NERC)
Sonia Mendonca (NERC)
Jeff Norman (MRO)
Jim Robb (NERC)
William Steiner (MRO)
Janet Sena (NERC)
Tasha Ward (MRO)

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

Midwest Reliability Organization (MRO)
CMEP Appendix 4A Audit

Background

The **Midwest Reliability Organization** (**MRO**) is one of six REs subject to the Electric Reliability Organization's oversight authority under a delegation agreement. MRO's offices are located in St. Paul, Minnesota. MRO's footprint includes approximately 224 registered entities consisting of municipal utilities, cooperatives, investor-owned utilities, a federal power marketing agency, Canadian Crown Corporations, and independent power producers.

The MRO region lies within the Eastern Interconnection and occupies upper Midwestern North America, covering 16 States, the Upper Peninsula of Michigan, as well as the Provinces of Saskatchewan and Manitoba in Canada. The MRO has all of the high-voltage direct current ties which connect the Eastern Interconnection to the Western Interconnection, and the Eastern Interconnection to the Texas Interconnection. MRO's approach to CMEP is characterized as a regulatory model that promotes Highly Effective Reliability Organizations ® (HEROs), which is intelligence led, risk-based and adaptive.

The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Program, which is required at least once every five years.

The MRO has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The audit objective was to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreements.

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of risk based CMEP, including the utilization of monitoring tools as defined within the ROP, or directed by NERC.

The MRO CMEP teams have established a strong framework from IRA, audit scoping to COP, and existence of communication routines to capture inputs from cross-functional teams. MRO teams demonstrated tremendous depth and breadth of expertise and rigor in the areas of Risk Assessment and Mitigation (RAM), Compliance Monitoring, and Enforcement. The risk based approach shared with Internal Audit entailed a focus on continent wide, region and

registered entity risks and inputs. In addition, review of the enforcement processing and disposition determination was adequately supported. Lastly, the primary monitoring tools utilized during the period under audit were compliance audits (50) and guided self-certifications (288). Self-certifications targeted specific CIP or O&P requirements across numerous, primarily higher to moderate at risk entities to provide more coverage of registered entity risk beyond formal audits.

During the course of our audit, we identified inconsistencies with the application of processes and utilization of tools. For example, Inherent Risk Assessment (IRA) and Compliance Oversight Plan (COP) processes and tools designed to ensure a holistic, consistent oversight strategy in order to determine the appropriate interval and CMEP Tool(s) for a registered entity, were primarily focused on higher to moderate inherent risk registered entities. These inconsistencies could prevent the RE from identifying common, aggregated risks within moderate to low inherent risk entities that adversely impact reliability.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
- Compliance Oversight Plans (COPs)
  - Internal Controls
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits
  - Spot Checks
  - Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security
  - Complaints and Investigations

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	1	0	1
Risk Assessment	0	1	0	1
COPs	0	1	0	1
Enforcement	0	0	0	0
Monitoring Tools	0	2	0	2
Supporting Activities	0	1	0	1
Total	**0**	**6**	**0**	**6**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	The Risk Assessment and Mitigation (RAM), Compliance Monitoring and Enforcement areas identify, apply and track required training in an ad hoc or inconsistent manner	Associates may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties
Medium	IRAs are not developed for all registered entities and the process to develop or update on a periodic basis largely relies on professional judgment and not a documented, repeatable methodology	Individual registered entity risk to the reliability of the bulk power system (BPS) are not identified, creating gaps with oversight strategy and inability to determine the appropriate interval and CMEP Tool(s)
Medium	COPs have been developed and/or updated based on three year entity audit requirements (i.e. BA, RC, TOP) and are inconsistent in the application to determine performance score, justification and relevant criteria	Inconsistent COP processes reduces the risk based application of the MRO regional monitoring program and may be perceived as unfair
Medium	The audit planning approach is primarily focused on three year entities and high risk entities with completed COPs as primary criteria, and audit scoping is often substantiated with institutional knowledge and/or professional judgement	Audit planning methodology does not provide coverage of all entities in a risk-based manner that factors in both performance characteristics and inherent risks. As a result, audit scoping may not address the most relevant risks to reliability.
Medium	Evaluation of registered entity internal controls is not evidenced prior to determination of eligibility for the self-logging program	The self-logging program is not administered consistent with risk based monitoring and establishing an environment of internal control awareness and proficiency by the registered entity
Medium	The RE did not require Periodic Data Submittals (PDS) in accordance with the schedule established by NERC, or on an as needed basis	Quantitative and qualitative analysis cannot be performed to ensure compliance or detect non-compliance with NERC Reliability Standards

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
1.	**Governance: Training**	**Enhance processes to ensure CMEP staff receive the appropriate training and learning programs timely** CMEP staff are required to be trained on processes and tools related to their area of responsibility. The Risk Assessment and Mitigation (RAM), Compliance Monitoring and Enforcement areas identify, apply and track required training in an ad hoc or inconsistent manner. • RAM utilizes an on the job and/or mentoring approach, and does not track the application or completion of required training • Training applicable or required is not formally evidenced across RAM, CM or Enforcement departments MRO CMEP staff may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties. Training process documentation, including requirements to provide training and track completion by applicable departments (functional and/or Human Resources) should be established.	September 30, 2022: Perform an internal review and document of required training for MRO CMEP staff. December 31, 2022: Create a process to track required training for CMEP staff. March 31, 2023: Implement process for CMEP staff to track mandatory training.	Regional Entity Director of Enforcement	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
2.	**Risk Assessment: Inherent Risk Assessment (IRA)**	**Develop Inherent Risk Assessments (IRA) and Compliance Oversight Plans (COP) for all registered entities to support risk-based CMEP** REs are required to perform an IRA of registered entities to identify areas of focus and the level of effort needed to monitor compliance with enforceable NERC Reliability Standards (Reliability Standards). The IRA is a review of potential risks posed by an individual registered entity to the reliability of the bulk power system (BPS). An assessment of BPS reliability impact due to inherent risk requires identification and aggregation of individual risk factors related to each registered entity based on what they own and operate. A representative sample of registered entities selected based on activity within the audit period, noted the following exceptions: • 2 of 12 (17%) did not have an IRA or COP performed since registration in 2018 and 2020 respectively, therefore would never be in consideration for inclusion in the audit plan. • 1 registered entity had an IRA, however it was performed in 2018 and no COP was performed. • One IRA (and COP) was developed that assessed three separate high risk registered entities in different states with varying risk criteria. The IRA was later identified as an MRRE audit. Per NERC guidance (NERC ERO Enterprise Coordinated Oversight Guide, March 2018), the Lead Regional Entity (LRE) is to create a consolidated IRA, with input from all Affected Regional Entity (ARE). No evidence of the ARE review and agreement of the finalized IRA was provided. Additionally, audit review of the IRA noted that only areas identified as appearing as a CMEP IP Risk Element or as a Risk Category were	December 31, 2022: Incorporate the schedule for completion/update of IRA's into an updated unified COP/IRA process for all MRO entities (see COP MAP below). This process will clearly identify the consideration of all requirements and not only those identified in a CMEP IP Risk Element or as a Risk Category. December 31, 2022: Incorporate upcoming RAPTF recommendations into our IRA process. We will insure that this update incorporates the need to clearly identify risk factors for each registered entity when consolidating multiple registered entities into one IRA for coordinated oversight. December 31, 2022: Ensure updated COP/IRA process includes documented approval from all associated Affected Regional Entities (ARE).	Regional Entity Director of Risk Assessment and Mitigation	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		included in the IRA, COP and scope. Documentation of individual risk criteria of the three registered entities was not evidenced. For example, one entity was noted as having unique BA Boundary Metering, RAS and synchronous condensers, none of which apply to the other two registered entities, however, consideration for those risk factors was not evidenced. • 9 of 12 (75%) registered entities selected were categorized as higher to moderate inherent risk, and there was no support for 3 (25%) registered entities deemed lower risk, which did not have an IRA and/or COP. An inconsistent approach to IRA/COPs may lead to gaps with oversight strategy and inability to determine the appropriate interval and CMEP Tool(s) for a registered entity. The risk based approach for IRAs is based on current or recent information from entity completion of MRO questionnaires, aligned to the ERO Enterprise guide category description of 1-4 (higher to moderate inherent risk) to determine the appropriate monitoring interval. In addition, NERC guidelines related to the creation of consolidated IRA should take into consideration a requirement to address unique risk factors. MRO should perform the IRA on a periodic basis, with the frequency based on a variety of factors including, but not limited to, newly registered entities, changes to a registered entity, and changes or additions to ERO Risk Factors.			

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
3.	**Compliance Oversight Plans (COPs)**	**Develop COPs consistently across all registered entities** The Electric Reliability Organization (ERO) Enterprise Guide for Risk-based Compliance Monitoring (Guide) describes the process used by the Regions to develop entity-specific COPs and serve as a common approach for the North American Electric Reliability Corporation (NERC) and MRO for implementing risk-based compliance monitoring. MRO develops a Compliance Oversight Plan (COP) to determine monitoring intervals and aid in determining the appropriate monitoring tool and applicable risk categories for a registered entity. COPs are developed by using results of the IRA (workbook and report) and performance considerations provided by Compliance Monitoring, RAM, Enforcement and Reliability Analysis and is one of multiple inputs used to scope MRO's oversight engagements. An IA review of COPs revealed the following: • COPs have been developed and/or updated based on three year entity audit requirements (i.e. BA, RC, TOP) and subsequently driven by the audit plan • RE did not adequately document the professional judgement, regarding specific risk criteria of a registered entity. For example, one entity, a registered Transmission Operator (TOP), was not assessed for Real Time Assessments (RTA), due to "the entity performing their own RTA". RTA have been the subject of concern, documented by a FERC and ERO Enterprise Joint Report outlining the importance of evaluating system conditions using Real-time data to assess existing and potential operating conditions. The report was based on a sampling of registered entities that were registered as Reliability Coordinators and/or Transmission Operators with responsibility for one or both Real-time Assessment	December 31, 2022: Develop a streamlined COP process for low inherent risk entities March 31, 2023: Develop a schedule to complete COPs for all MRO entities MRO will continue to work with the NERC RAPTF to develop consistent tools and approaches to performing COPs and assessing performance data. Within two quarters after the ERO RPMG/RAPTF approves performance criteria, MRO COP input owners will develop procedures and tools using the approved approach.	Regional Entity Director of Compliance Monitoring	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		Requirements(s). The sample represented diversity in size, region and responsibility, as well as large, mid-sized and small Transmission Operators. • Inconsistent utilization of performance data and criteria in developing the COP. Inconsistent processes reduces the effectiveness of the risk based application of the MRO regional monitoring program and reduces the quality and appropriate risk oversight of the registered entity. Establish criteria to substantiate determinations and provide evidence that each registered entity is handled consistently and fairly.			
4.	**Monitoring Tools: Audit Plan/Scoping**	**Apply audit planning and scoping methodology holistically and consistently** Compliance audits should be planned and scoped based on risk assessment processes and informed inputs such as an IRA, COP, performance data, culture of compliance, internal controls, self-certification results, and ROP requirements (i.e. 3 year audits of BA, RC, TOP…), demonstrating a risk-based approach. MRO audit planning methodology does not provide coverage of all entities in a risk-based manner. The planning process is to identify ROP three year entities for the upcoming year, review those entities with a completed COP, and lastly, apply 'institutional knowledge' to judgmentally select entities. This process omits all entities that do not have a completed COP, appearing exclusive to those that are moderate to low risk. Documentation was not evidenced to support the methodology or decision making process to include performance data in the scoping of audits. In addition, manager review (CIP/O&P) of audit scoping is not a documented	December 31, 2022: Develop guidance and improve the tools used for management approval of audit scopes. December 31, 2022: Develop a long term audit planning methodology and supporting tools. December 31, 2023: Develop a long term plan (5 to 6 years) using the long term audit planning methodology and tools In addition, MRO will continue to work with the ERO Enterprise to develop consistent tools and approaches to performing audit planning activities.	Regional Entity Director of Compliance Monitoring	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		process supported by rationale or justification for standards in scope. Audit planning and scoping may not provide risk-based coverage to the monitoring frequency defined from the ERO Enterprise oversight and categorization strategy, or address specific registered entity engagement risks to ensure reliability through an effective CMEP. The audit planning approach focuses on three year entities, high risk registered entities, and related COPs as primary criteria, and audit scoping is reliant on institutional knowledge and/or professional judgement. Document audit methodologies for planning and scoping audits to ensure coverage is adequate to address risks across the Region, and audit engagements appropriately address the most relevant risks and potential control issues.			
5.	**Monitoring Tools: Self Logging**	**Administer the Self-Logging Program consistent with the objectives of the monitoring tool and Rules of Procedure** Consistent with the Rules of Procedure and Appendix 4C 3.5A, the Regional Entity should perform a formal review of internal controls, and may grant a registered entity eligibility to log non-compliance posing minimal risk to the BPS. Specifically, analysis of a registered entity's ability to sufficiently demonstrate they have institutionalized processes to identify, assess and correct non-compliance should be evidenced. Documentation was not provided by the registered entity to the RE for the registered entities sampled (5). The RE executed their own questionnaire as criteria to determine eligibility.	June 30, 2023: After the completion of NERC CMEP audits of the six regional entities, engage NERC and the regions in establishing more formal criteria and guidance on what constitutes a "formal review of internal controls" of an entity's ability to identify, assess, and correct. September 30, 2023: Modify MRO's procedures to be consistent with new ERO approach December 31, 2023: Implement new self-logging program and, in	Regional Entity Director of Enforcement	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		The self-logging program is not administered consistent with risk based monitoring and establishing an environment of internal control awareness and proficiency by the registered entity. Eligibility for the self-logging program should contain an analysis of a registered entity's ability to sufficiently demonstrate they have institutionalized processes to identify, assess and correct non-compliance, and retained by the RE to support overall conclusions.	consultation with NERC, determine whether entities previously admitted into MRO's self-logging program should undergo a re-evaluation.		
6.	**Monitoring Tools: Periodic Data Submittals (PDS)**	**Provide Periodic Data Submittals in accordance with established schedules** The Compliance Enforcement Authority (CEA) requires PDS in accordance with the schedule stated in the applicable Reliability Standards, as established by the CEA, or as-needed, in accordance with the NERC ROP, Appendix 4C – Section 3.6. The RE did not require PDS in accordance with the schedule established by NERC, or on an as needed basis • TPL 007-4, CIP 14-2, and CIP 008-6 were identified for PDS during the period under audit Quantitative and qualitative analysis cannot be performed to ensure compliance or detect non-compliance with reliability standards. The RE should ensure the personnel responsible for PDS is aware of, establishes and documents controls, applicable to the periodic data submittal posted by NERC on the NERC Compliance One-Stop Shop, or as referenced within the annual CMEP IP.	December 31, 2022: Consolidate MRO's PDS program into one department. December 31, 2023: Update MRO's PDS tools and procedures to ensure PDS are performed timely and consistently.	Regional Entity Director of Compliance Monitoring	Medium

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment C

Appendix 4A Audit Report – Northeast Power Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

Northeast Power Coordinating Council (NPCC)

Date: August 4, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Charles Dickerson, President & CEO, NPCC

From: NERC Internal Audit

Date: August 4, 2022

Subject: Regional Entity CMEP 4A Audit – Northeast Power Coordination Council (NPCC)

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity Compliance Monitoring and Enforcement Program (CMEP Appendix 4A) Audit of NPCC.

The audit objective is to assess NPCC's implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, Appendix 4C, the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreement.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: **Arthur Brown**
Manny Cancel
Ben Eng
Damase Hebert
Kelly Hanson
Jackie Jimenez
Mark Lauby
Scott Nied
Sonia Mendonca
Jim Robb
Janet Sena
Jason Wang

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

NPCC

CMEP Appendix 4A Audit

Background

NPCC is one of six Regional Entities subject to the Electric Reliability Organization's oversight authority under a delegation agreement. NPCC's offices are located in New York, New York. NPCC has approximately 236 registered entities consisting of municipal utilities, cooperatives, investor-owned utilities, and independent power producers.

The NPCC geographic region includes the State of New York and the six New England states as well as the Canadian provinces of Ontario, Québec and the Maritime provinces of New Brunswick and Nova Scotia. Overall, NPCC covers an area of nearly 1.2 million square miles, populated by more than 55 million people.

The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Monitoring and Enforcement Program, which is required at least once every five years.

NPCC has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of the risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC.

From the outset of this audit, NPCC leadership expressed an openness to the audit and a willingness to receive observations and recommendations to enhance its operations. NPCC fosters an environment that enables continuous improvement.

The primary monitoring tools used during the period under audit were Compliance Audits (covering 62 registered entities) and Self-certifications with 57 CIP and 5 O&P completed in 2021. NPCC utilizes the Master Monitoring Schedule spreadsheet to give each Registered Entity in their footprint a risk category and a monitoring interval.

Since 2020, the NPCC methodology calls for the development of Compliance Oversight Plans (COPs) for all entities on the audit schedule, in advance of the audit. As a result, COPs have been developed for approximately 64 or 27% of the entities within the RE footprint. The COP is an essential component of risk-based CMEP and assists in the consistent administration of the ERO Oversight Strategy. Therefore, without the existence of a COP, compliance monitoring activities are potentially incomplete, or established with ineffective intervals to proactively address and mitigate risks.

NPCC has 22 Full Time staff (FTEs) dedicated to Compliance Monitoring, Enforcement and Entity Risk Assessment activities. This equates to roughly half the average number of FTEs (43) of the other five Regional Entities. With increasing noncompliance activity across the US and the varied, complex governance models across the Canadian provinces, NPCC is facing challenges to stay ahead of the growing volume of potential noncompliance in their Region. NPCC has recognized this trend and has budgeted for CMEP Staff to grow to 28 FTEs in the 2023 BP&B. Requests for additional CMEP resources are expected to occur in 2024 and 2025.

The demands of CMEP activities are unrelenting, as registered entities continue doing their part to identify, report, and mitigate noncompliance. NPCC should maintain its commitment to continuous improvement to ensure it adequately allocates its limited resources to the activities that assure the effective and efficient reduction of risks to the reliability and security of the BPS.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
- Compliance Oversight Plans (COPs)
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits
  - Internal controls
  - Spot Checks
  - Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	0	1	1
Risk Assessment	0	3	0	3
COPs	0	1	1	2
Enforcement	0	1	0	1
Monitoring Tools	0	2	1	3
Supporting Activities	0	1	0	1
Total	**0**	**8**	**3**	**11**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	Open Enforcement Actions (OEAs) are not processed timely to address risk of non-compliance with the appropriate disposition and action	Unprocessed OEAs increases risk to BPS. Lack of transparency to all Open Enforcement Actions prevents complete assessment of entity risk and mitigation.
Medium	Compliance Audits are not conducted as planned	Continued focus on prior year audits may increase the risk of delays to the current year audits as well as not identify risks and potential noncompliance in a timely manner.
Medium	IRA/COPs have not been developed for a majority of registered entities within the footprint and IRA/COP process lacks flexibility to fully support a risk-based approach	Incomplete or inaccurate identification of assets to apply required reliability standards and the appropriate monitoring interval and tools to mitigate risks to BPS.
Low	IRA/COP results lack continuity to audit scope	Risk-based audit scope is not adequately explained. Registered entity and outside observers may not have clear understanding of rationale for all Reliability Standards included in the scope.
Medium	Mechanism for periodic risk assessment with entities is not timely to support annual audit planning	Annual audit planning process is ineffective without a current risk assessment.
Medium	Annual audit planning is not formally documented with support of entity risk assessment factors to ensure coverage of relevant risks and related reliability standards.	The annual audit plan does not sufficiently address the most current risks.
Medium	CMEP Policies and Procedures are not developed and in some cases have not been updated.	Risk-based approach to CMEP is not administered through documented and routinely updated policies and procedures.
Medium	Current risk assessment and audit planning processes do not address two-year gap with the execution of CIP-014 audits as a result of pandemic conditions.	Increased likelihood of CIP-014 non-compliance with reliability standards may adversely affect the BPS.

Low	A process outline does not exist to support and assist employees with understanding and execution of the Conflict of Interest (COI) Policy	Misunderstanding and interpretation of COIs exist and inaccurate or unfavorable responses are not effectively identified and resolved.
Medium	Offsite Audits are designed to be executed with limited interaction and without interviewing registered entity personnel, demonstrating a self-certification approach versus audit	Lack of audit techniques, such as direct questioning via interviews, may hamper auditors understanding of processes and associated internal controls, increasing the risk of inaccurate conclusions.
Medium	Audit work programs are not consistently developed to assess an entity's internal controls prior to the start of audit Fieldwork per NERC guidance and audit standards (i.e. IIA/IPPF)	Inconsistent assessment of internal controls reduces the effectiveness of risk-based CMEP.

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
1.	**Enforcement** **App 4C – Section 3.0, 3.8 and 5.0, 5.1 and 5.2.** **NERC ROP Section 403 - Required attributes of RE CMEP; 403.5 Program Resources - RE Compliance Staff**	**Open Enforcement Actions (OEAs) are not processed timely to address risk of noncompliance with the appropriate disposition and action. (Self-Identified)** The volume of OEAs has been increasing the past few years to the point where NPCC had 552 open on April 1 2022. The breakdown of which year they originated is as follows: 2019: 48 2020: 159 2021: 280 2022: 65 **Total: 552** Preliminary Screens are processed according to process (Section 3.8) however, many of those determined to be Minimal Risk, via the Initial Triage Process, are not processed timely as Compliance Exceptions. NPCC attributes their inability to keep pace with the increasing numbers of noncompliance to resource constraints. With no timetable represented to ensure complete processing, there is increased	1. NPCC will advance the plan to hire additional FTE's for enforcement. Specifically, NPCC plans to onboard two to three new FTEs in 2022 to assist in enforcement. This will result in 7 to 8 FTE's to work on enforcement issues (up from 5 historically). 2. NPCC will evaluate and consider whether to request additional FTE's for the 2024 and 2025 Business Plans and Budgets. 3. NPCC will develop enforcement approaches designed to streamline the processing of	December 31, 2022 June 30, 2023 December 31, 2022	Regional Entity Manager, Enforcement and Regional Entity Associate General Counsel, Director Enforcement Regional Entity Associate General Counsel, Director Enforcement All enforcement staff	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		risk associated with non-processed PNCs including: • Potential of repeat or recurring violation of Reliability Standards • Lack of visibility hampers the complete view of the entity risk profile and increases reliability and security risk to the BPS. NPCC should review the current and prospective Enforcement personnel resource model to ensure: 1) proper review all OEAs in the pipeline and 2) determine a sustainable approach in the future to identify and process PNCs timely, and apply the required monitoring strategy and interval.	commonly violated Standards and document all the steps within the processing.			
2.	**Compliance Monitoring** **NERC ROP Section 403 - Required attributes of RE CMEP; 403.5 Program Resources - RE**	**Compliance Audits are not all completed in the calendar year of the plan.** IA testing performed in mid-May 2022, identified 4 of 16 (25%) 2021 compliance audits were still in progress. Audit Notification Letter's (ANL's) for 2 of 4 indicated the audits did not commence until 2022. As of May 17, 2022, NPCC asserted that 9 of 22 (41%) of the 2021 Compliance audits were not yet completed.	NPCC has as a matter of practice, accepted a degree of off-site completion overlap between years. The 2023 annual audit plan that will be developed in 3rd/4th quarter 2022 will take into consideration previous historical	October 31, 2022 (when 2023 annual plan is developed)	Regional Entity Director, Compliance Monitoring	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		As a practice, the majority of audits should be completed during the calendar year. Audit execution delays may increase the risk of noncompliance not being detected timely, and/or determining the proper monitoring interval as a result of the executed audit In addition, increased back log of prior year audits may increase the risk of delays to current plan year audits. NPCC leadership cited the continuous requests from registered entities to extend or delay audit start dates as a practice they honor, and in some cases honor several requests. NPCC should ensure that Compliance Audits are executed within the plan year to adequately support auditor resource planning, and consider evaluating other performance criteria to support extensions as requested from the registered entities to delay the audit start date. This practice may reduce the back log, and ensure that audit staff is equipped to execute audits as planned	delays that will result in a 2023 annual plan that will more accurately align with actual capabilities to complete a finite quantity of off-site audits in the 2023 calendar year.			

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		within the appropriate monitoring interval.				
3.	**COPS**	**COPs have not been developed for a majority of registered entities within the footprint and IRA/COP process lacks flexibility to fully support a risk-based approach** At current, 64 of 236 (27%) of registered entities within the NPCC footprint have a completed COP. NPCC's approach since 2020 is to complete the IRA/COP process for each entity on the annual audit plan and to complete others, time permitting. Per NERC ROP and ERO Enterprise oversight strategy and CMEP tool interval guide, an Inherent Risk Assessment should be developed as the first step to determine what assets are owned by the registered entity and associated Reliability Standards required to comply. Further, Regional Entity staff should develop IRAs and COPs in accordance with the defined oversight strategy to determine the appropriate CMEP tool(s) for a registered entity.	CMEP candidate search is ongoing as NPCC is budgeted for 25 CMEP FTE in 2022 and 28 CMEP FTE for 2023. To ensure NPCC COP mitigation will align with ERO COP expectations, NPCC will coordinate the RPMG (and the RAPTF) for agenda item discussions to reconfirm NERCs uniform direction to the Regions on the development of COPs and possible adjustment of the top 5 rule as needed. NPCC will add words to CI-22 IRA and CI-23 COPs to allow for additional Staff	December 31, 2022 September 30th and December 31, 2022 RPMG/RAPTF meetings September 30, 2022	Regional Entity VP, Compliance Regional Entity Manager Entity Risk Assessment Regional Entity Manager	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		The IRA/COP process lacks flexibility to support a risk-based approach. Specifically: NPCC utilizes the following calculation to determine a weighted percentage for each Risk Category: **NPCC IRA Tool identified RSs / Total ERO RSs for a specific risk category** Once the percentages are assigned, NPCC applies the "Top 5" rule where 5 and only 5 Risk Categories are selected. This rule lacks flexibility to support a risk-based approach. In addition, there does not appear to be the opportunity to override using professional judgement to alter results within the methodology. There is no ability to utilize professional judgement by overriding statistical calculations built into the COP process or to deviate from the "Top 5" rule. The Oversight Strategy was not consistently documented within the COP report and there was insufficient evidence to validate the overall target monitoring interval. Overall, the current IRA/COP process may not correctly identify to NPCC and to the	flexibility and professional judgment.		Entity Risk Assessment	

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		entity the Reliability Standards which present the greatest risk to the BPS. An increase in Entity Risk Assessment personnel would likely increase NPCC's capability to: • Build flexibility to support a risk-based approach to the IRA/COP process • Complete IRA/COPs for a greater percentage of Registered Entities overall, modeling risk-based CMEP.				
4.	**COPS**	**IRA/COP results lack continuity to audit scope** As significant time is taken to prepare the IRA/COP and the COP is shared with the entity, entities are given a roadmap as to the population of Reliability Standards which were considered to be included in the scope of their audit. However, our analysis identified several audits where the scope included Reliability Standards which are not included in the COP. In some cases, our testing noted Reliability Standards listed in the IRA which were not included in the output of the COP, however these same Reliability	To ensure NPCC COP mitigation will align with ERO COP expectations, NPCC will coordinate the RPMG (and the RAPTF) for agenda item discussions to reconfirm NERCs uniform direction on the development of COPs, Appendix B in the COP, the relation to audit scope, and to discuss consistent inclusions of enhanced	December 31, 2022	Regional Entity Manager Entity Risk Assessment	Low

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		Standards were included in the audit scope. With no explanation for the inclusion of RSs in the scope, which were not included in the COP, the credibility of the IRA/COP process may be challenged. A clear explanation of why certain Reliability Standards, which were not included in the COP, but were included in the Scope would provide improved continuity and help support confidence in the credibility of the IRA/COP process. Further, our testing of the IRA/COP process identified 4 of 15 samples, which did not have a completed COP prior to the issuance of the Audit Notification Letter (ANL). A review of the IRA/COP process to identify opportunities to strengthen the continuity/transparency of Reliability Standards being evaluated and ultimately selected for the scope, would enhance the credibility of the IRA/COP process.	explanation to the entity. NPCC will add words to CI-22 and CI-23 to allow for Staff flexibility and to include enhanced explanations.	September 30, 2022	Regional Entity Manager, Entity Risk Assessment	

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
5.	**Risk Assessment** **NERC ROP Section 403 - Required attributes of RE CMEP; 403.5 Program Resources - RE Compliance Staff**	**Mechanism for periodic risk assessment with entities is not timely to support annual audit planning** NPCC does not have a mechanism (i.e., Entity Profile Questionnaire) in place to receive timely updates from their entities in order to support the annual audit planning process. ***IIA Standard 2010.A1*** *– The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually.* Our analysis demonstrates more than 50% of the entities have not provided an updated IRA since 2016. NPCC should have an annual process to check in with their entities to get a summary of any significant changes which have occurred. Without timely updates, NPCC may not have the most relevant entity information to utilize to conduct their risk assessment in support of the annual audit planning process.	CMEP candidate search is ongoing as NPCC is budgeted for 25 CMEP FTE in 2022 and 28 CMEP FTE for 2023. NPCC will develop a plan to conduct annual communications to all entities to remind them of their obligations to update NPCC for changes that may affect their IRA.	December 31, 2022 September 30, 2022 Method for enhanced annual communication decided upon and implemented September 30, 2022	Regional Entity VP Compliance Regional Entity Manager, Entity Risk Assessment	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		NPCC has a smallest CMEP staff among the regions. Resources have not been assigned to gather an update for each entity on an annual basis.				
6.	**Risk Assessment** **NERC ROP Section 403 - Required attributes of RE CMEP; 403.5 Program Resources - RE Compliance Staff**	**Annual audit planning is not formally documented with support of entity risk assessment factors to ensure coverage of relevant risks and related reliability standards.** NPCC audit planning includes the selected the 3 year audits (as per ROP) which are due for the year and then applies professional judgement for the remaining 219 entities without evidence of a documented risk based evaluation for the entities. IA was unable to evidence documentation which supports the risk evaluation of each entity. NPCC Master Schedule nor any other tools were available, which contained: performance data, compliance history, and internal controls, etc, which would be expected to be available for inclusion in the risk evaluation. **ROP 3.1.4 Scope of Compliance Audits** states:	CMEP candidate search is ongoing as NPCC is budgeted for 25 CMEP FTE in 2022 and 28 CMEP FTE for 2023. To ensure NPCC Risk Assessment mitigation will align with ERO COP expectations, NPCC will coordinate the RPMG (and the RAPTF) for agenda item discussions to reconfirm NERCs uniform direction on performing risk assessments and resulting audit scopes to understand opportunities to enhance audit planning actions	December 31, 2022 December 31, 2022	Regional Entity VP Compliance Regional Entity Manager Entity Risk Assessment	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		Regional Entities will tailor the final scope of any Compliance Audit based on the results of the Registered Entity's Inherent Risk Assessment and, if applicable, taking into consideration the results of an Internal Controls Evaluation. Without documented support for the risk evaluation there is increased risk the annual audit plan may not reflect what management intended. NPCC has not had resources to support the development of automated tools to help provide the information needed to adequately support the annual audit planning process. Going forward, additional resources should be dedicated to provide the needed tools to support the annual audit planning process.	(including acquiring CMEP technology solutions) that were identified in these 6 Regional audits and then document the new processes.			
7.	**Supporting Activities**	**CMEP Policies and Procedures are not developed and in some cases have not been updated** Policies and procedures are not documented, or have not been updated in a timely manner. These include: • Complaints and Investigations procedures are not documented.	NPCC will develop a procedure for complaints and investigations. NPCC will update the Enforcement manual to include changes to account	September 30, 2022 September 30, 2022	Regional Entity Associate General Counsel, Director Enforcement	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status

		• NPCC Enforcement Manual version 2.0 (last updated 10/17/2019).
		  ○ Changes to account for the implementation of Align as well as organizational changes were not reflected
		  ○ Triage process is not documented
		• Within the Compliance Oversight Plan CI-23 Rev 3, there is not a concise methodology for assignment of: Minimal, Moderate and Serious ratings.
		• NPCC includes their own risk elements into an NPCC CMEP IP each year – this is only partially documented in CI-22.
		
		Procedures should be reviewed/updated whenever significant changes occur or at least annually.
		
		Without clearly documented policies and procedures the Regional activities may not be as management intended.
			for the implementation of Align, organizational changes, and documentation of the procedure for the Triage process.
			
			NPCC will update the methodology for assignment of ratings in CI-23.
			
			NPCC will fully document inclusion of risk elements into an NPCC CMEP IP in CI-22.
			
			As NPCC policies and procedures are updated, NPCC will implement and use a Governance, Risk, and Compliance tool to ensure that each policy and procedure is reviewed for updates at least annually.
				
				September 30, 2022
				
				September 30, 2022
				
				September 30, 2022
					Regional Entity Enforcement Attorney
					
					Regional Entity Manager, Entity Risk Assessment
					Regional Entity Manager, Entity Risk Assessment
					
					Regional Entity Associate General Counsel, Director Enforcement	

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
8.	**Compliance Monitoring** **NERC ROP Section 403 - Required attributes of RE CMEP; 403.5 Program Resources - RE Compliance Staff**	**Current risk assessment and audit planning processes do not address two-year gap with the execution of CIP-014 audits as a result of pandemic conditions** CIP-014 audits require that procedures and evidence be executed on-site/on-premise. However, due to pandemic related conditions, CIP-014 was not audited in 2020 and 2021, and NPCC has no plans to make up the audits. Alternatively, the registered entities scheduled in 2020 and 2021 will be evaluated in the next auditing cycle. Since there has been a two-year gap, NPCC should prioritize the CIP-014 audits and conduct them as soon as possible rather than waiting for the next auditing cycle. In addition, with the recently approved revisions to the ROP related to CIP-014, there is flexibility to conduct the audits through other methods or procedures versus strictly on-site. Without conducting the CIP-014 audits, noncompliance with CIP-014 may not be identified for several years, increasing the risk to the bulk power system.	NPCC is including CIP-014 in 2022 TO/TOP audit scope for remote audits and on-site audits. The inclusion of CIP-014 for remote audits began in May 2022 and will continue in-person upon our return to on-site audits in October 2022. CMEP candidate search is ongoing as NPCC is budgeted for 25 CMEP FTE in 2022 and 28 CMEP FTE for 2023.	June 30, 2022 October 31, 2022 December 31, 2022	Regional Entity VP, Compliance; Regional Entity Director Compliance Monitoring Regional Entity VP Compliance	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		NPCC has the smallest CMEP staff comparatively amongst all the Regional Entities. Resources have not been assigned to perform CIP-014 audits due to availability of resources and priorities established by NPCC leadership. NPCC should evaluate and prioritize CIP-014 audits using a risk-based approach.				
9.	**Governance**	**A process outline does not exist to support and assist employees with understanding and execution of the Conflict of Interest (COI) Policy.** Question number 2 from the NPCC COI disclosure is not clear. The policy question states: "Please list any entities in the electricity sector in which you, or any relative/ family member, or any member of your immediate household, have a direct or indirect financial interest. You need not list diversified mutual funds that may have electricity sector holdings. Please indicate whether the equity or other ownership/beneficial interest in such entities (as a percentage) is in excess of 5%."	NPCC staff will review the COI Policy and annual questionnaire and develop recommended edits or a procedure to assist staff with understanding and executing the COI Policy.	December 31, 2022	Regional Entity Associate General Counsel, Director Enforcement	Low

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		NPCC reported there was confusion concerning what the 5% is in reference to, such as an individual's portfolio or 5% of the outstanding company stock? Other questions were raised concerning whether other criteria need to be considered. For example: • Is less than 5% acceptable, or should all be disclosed and required to divest? • Should affiliates of the entity be considered? The COI policy should be reviewed with intent of clarifying specifics about what constitutes a COI, and consistently apply the policy and ensure the correct interpretation and understanding.				
10.	**Compliance Monitoring**	**Offsite Audits are designed to be executed with limited interaction and without interviewing registered entity personnel, demonstrating a self-certification approach versus audit** For RA, BC and TOPS, NPCC utilized an "onsite" audit approach. During the pandemic "onsite" audits were conducted remotely but did include interviews. For the remainder of the	NPCC recognized the benefit of this prior to the NERC CMEP audit and started in 2022 to include an interview aspect in the NPCC off-site audits.	September 30, 2022	Regional Entity Director, Compliance Monitoring	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		registered entity audits on the audit plans for 2020 and 2021, NPCC conducted "offsite" audits. For "offsite" audits, it was NPCC's intention to execute the monitoring activity while minimizing interviews, relying instead on the use of Request for Information (RFI), where possible. When NPCC felt there was a lack of information from the RFI(s), NPCC did conduct interviews. Lack of audit techniques, such as direct questioning via interviews, may hamper auditors understanding of processes and associated internal controls, increasing the risk of incomplete or inaccurate conclusions. In addition, the audit approach may be perceived as less credible or unfair by the registered entity due to the lack of interaction or participation in the audit. NPCC asserts that as of 2022, the procedures for Offsite audits now include interviews and other widely accepted audit techniques				

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		NPCC should develop a consistent approach to planning and executing Offsite audits with the appropriate audit techniques and procedures that include participation from the auditee.				
11.	**Risk Assessment**	**Audit work programs are not consistently developed to assess an entity's internal controls prior to the start of audit Fieldwork per NERC guidance and audit standards (i.e. IIA/IPPF)** IIA Standard **2240.A1**- Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly. The intent to perform an evaluation of the registered entity's internal controls is not appropriately evidenced prior to the commencement of the audit fieldwork. In 2020, Reliability Standard Audit Worksheet (RSAWs) did not include the results of an evaluation of internal controls. While a number of reviews included internal controls in 2021, the approach was inconsistent overall.	In 2022, NPCC began using the NERC ICAT form and familiarizing our way through the use of the form with the other Regions. This will help us with documenting a "plan" of what controls we need to focus on understanding/assessing during the forthcoming audit. Improving our proficiency in the use of the ICAT will also help us with memorializing in sufficient fashion the results of the controls assessment aspect of the	September 30, 2022	Regional Entity Director, Compliance Monitoring; Regional Entity Manager, Entity Risk Assessment	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Status
		A work program which documents the expected controls should be reviewed and approved prior to the commencement of fieldwork. The inclusion of internal controls on RSAW going forward should formulate a more informed assessment of the registered entity as fieldwork begins.	completed audit engagement.			

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment D

Appendix 4A Audit Report – ReliabilityFirst

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

ReliabilityFirst (RF)

Date: June 27, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Tim Gallagher, President & CEO, ReliabilityFirst

From: NERC Internal Audit

Date: June 27, 2022

Subject: Regional Entity CMEP 4A Audit – ReliabilityFirst (RF)

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity Compliance Monitoring and Enforcement Program (CMEP Appendix 4A) Audit of ReliabilityFirst.

The audit objective is to assess ReliabilityFirst's implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, Appendix 4C, the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreement.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Manny Cancel
Jeff Craigo
Kelly Hanson
Erik Johnson
Mark Lauby
Sonia Mendonca
Marcus Noel
Jim Robb
Niki Schaefer
Janet Sena
Kristen Senk
Matt Thomas

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

ReliabilityFirst
CMEP Appendix 4A Audit

Background

ReliabilityFirst (RF) is one of six Regional Entities subject to the Electric Reliability Organization's oversight authority under a delegation agreement. ReliabilityFirst's offices are located in Cleveland, Ohio. ReliabilityFirst members include approximately 266 registered entities consisting of municipal utilities, cooperatives, investor-owned utilities, and independent power producers.

The ReliabilityFirst region is situated in the Eastern Interconnection and stretches from Lake Michigan to the Eastern Seaboard and includes all or portions of Delaware, New Jersey, Pennsylvania, Maryland, Virginia, Illinois, Wisconsin, Indiana, Ohio, Michigan, Kentucky, West Virginia, Tennessee and the District of Columbia and includes several large/dense urban areas including: Chicago, Cleveland, Detroit, Pittsburgh, Philadelphia, and Baltimore.

The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Monitoring and Enforcement Program, which is required at least once every five years.

ReliabilityFirst has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of the risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC.

ReliabilityFirst's commitment to the reliability and security of the bulk power system is well demonstrated across its CMEP activities. At the outset of this audit, ReliabilityFirst leadership expressed an openness to the audit and a willingness to receive observations and recommendations to enhance its operations. ReliabilityFirst fosters an environment that enables innovation and continuous improvement.

For the period under audit and based on our representative sampling, RF's compliance monitoring meets the requirements of the ROP Section 400, Appendix 4C, annual CMEP IP, and the delegation agreement.

The primary monitoring tools used during the period under audit were Compliance Audits (covering 58 registered entities) and Spot Checks (covering 38 registered entities). ReliabilityFirst used CIP Self-Certifications to target registered entities with Low Impact BES Cyber Systems to provide more coverage of registered entity risk beyond

formal audits. In addition, ReliabilityFirst has developed templates to facilitate Compliance Oversight Plans for groups of registered entities, such as wind farms, that share common characteristics and risk considerations. By completing Inherent Risk Assessments for all but its newest registered entities, ReliabilityFirst established a foundation for risk-based compliance monitoring that guides its oversight strategies.

The demands of CMEP activities are unrelenting, as registered entities continue doing their part to identify, report, and mitigate noncompliance. ReliabilityFirst should maintain its commitment to continuous improvement to ensure it adequately allocates its limited resources to the activities that assure the effective and efficient reduction of risks to the reliability and security of the BPS.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
  - Internal Controls
- Compliance Oversight Plans (COPs)
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits
  - Spot Checks
  - Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	0	0	0
Risk Assessment	0	0	0	0
COPs	0	1	0	1
Enforcement	0	1	0	1
Monitoring Tools	0	0	1	1
Supporting Activities	0	0	0	0
Total	**0**	**2**	**1**	**3**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	Self-logged PNCs not reported in a timely manner	The self-logging program is not administered consistent with risk based monitoring and in accordance with the FERC regulations, 18 C.F.R. Section 39.7 (b). Potential non-compliance or aggregated themes are not detected timely by NERC/FERC periodic reviews.
Medium	Lack of an ERO Enterprise-wide IRA/COP methodology to determine registered entity risk rating and consequent monitoring frequency	Inaccurate registered entity risk rating and consequent monitoring frequency are not aligned with registered entity's inherent risk.
Low	Lack of communication for reliability standards included in the audit scope which were not in the COP	Risk-based audit scope is not adequately explained. Registered entity and outside observers may not have clear understanding of rationale for all Reliability Standards included in the scope.

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
1.	**Enforcement**	**Self-logged PNCs not reported in a timely manner.** For a sample of Self-logs reviewed during the audit, we identified instances prior to the implementation of Align where ReliabilityFirst received the Self-logs and did not record them in CDMS as noncompliance for reporting to NERC and FERC until Enforcement personnel processed the noncompliance. The management practice at ReliabilityFirst was to enter self-logged issues into CDMS once they had determined the issue would be resolved as a Compliance Exception. FERC regulations, 18 C.F.R. Section 39.7(b), require Regional Entities to have procedures to report promptly to the Commission any self-reported violation. As PNCs were not being entered promptly into CDMS, NERC and FERC were not notified until after the disposition was processed as a Compliance Exception. Internal Audit expanded the sample to include self-logged issues since the implementation of Align, where it was validated that the date RF submitted the noncompliance to NERC matches the date RF was notified of the noncompliance through a Self-log submission. This process appears to eliminate the delay by real time entry and submission in Align.	ReliabilityFirst believed it was complying with 18 C.F.R. Section 39.7(b) and CMEP self-logging requirements by reporting minimal risk self-logs at the time of disposition and was always transparent with NERC and FERC regarding this process. Regarding management actions needed to address this observation, ReliabilityFirst's reporting of self-logs changed with the implementation of Align. Registered Entities now submit self-logs directly into Align, which triggers screening and notification to NERC based on design elements of the Align system. Therefore, this observation is historical in nature, and no additional management actions are needed.	Regional Entity Director, Legal and Enforcement	Medium
2.	**Compliance Oversight Plans (COPs)**	**Lack of an ERO Enterprise-wide IRA/COP methodology to determine registered entity risk rating and consequent monitoring frequency**	There was no ERO Enterprise wide IRA/COP methodology in place during the period of the observation, and therefore ReliabilityFirst created its own methodology, which was	Regional Entity Director, Reliability Analysis	Medium

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		For much of the audit period, the ERO Enterprise had not established a single methodology for the Regional Entities to use to develop Compliance Oversight Plans that incorporated the risk ratings from the Inherent Risk Assessment of the registered entity. There was no meaningful differentiation among the ERO Risk Factors that comprised the Inherent Risk Assessment. As such, our audit identified instances where a lower risk rating was determined. In addition, one entity was rated High in 11 of 18 Risk Factors, however, since six of the Risk Factors did not apply to the registered entity,[1] the overall calculation of the entity's risk was in the range that ReliabilityFirst had established for a Moderate risk registered entity. Establishing a monitoring frequency that does not correspond to a registered entity's inherent risk may increase risks to reliability as a result of reduced monitoring by the Regional Entity. Lack of an ERO methodology with sufficient detail resulted in ReliabilityFirst developing an IRA/COP process which in some cases during 2020 led to a lower rating than under the updated process introduced in the second half of 2021. During 2021, the ERO Enterprise implemented an updated IRA/COP process, wherein several of the ERO Risk Factors are considered Primary Risk Factors. If a registered entity is scored as High in any of those Primary categories, the	shared with NERC and the other Regions. ReliabilityFirst notes that the IRA risk rating is one input of many when determining monitoring frequency, and ReliabilityFirst staff used professional judgment to determine the appropriate monitoring frequency for the entity referenced in the observation. This entity had compliance monitoring engagements each year from 2015-2021, demonstrating that ReliabilityFirst monitored the entity appropriately and commensurate with the inherent risk posed. Regarding management actions needed, in 2020, in the spirit of continuous improvement, the ERO Enterprise implemented an updated IRA/COP process (described within the observation) which addresses the identified issue. Therefore, this observation is historical in nature, and no		

[1] Most of ReliabilityFirst's footprint is composed of markets that do not have vertically-integrated utilities owning transmission and generation under a single registered entity.

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		registered entity would be ranked as a Higher inherent risk with more frequent monitoring. Going forward, when the ERO Enterprise is establishing processes for all of the Regional Entities, developing a single, documented approach for use across all of the Regional Entities, as early as practical, can promote consistency in application of processes.	additional management actions are needed.		
3.	**Compliance Monitoring Processes and Tools**	**Lack of communication for reliability standards included in the audit scope which were not in the COP** During a review of a sample of six IRA/COP's, two audit scopes included Reliability Standards that were not included in the COP. The audit report did not explain the rationale for inclusion of these reliability standards in the scope. Audit scope can legitimately include requirements not in the COP. For example, new versions of Reliability Standards may become effective (*e.g.*, CIP-003-7 for Low Impact BES Cyber Systems) and/or prioritized for monitoring (*e.g.*, CIP-008, based on the low rate of reporting of attempts to compromise BES Cyber Systems) after completion of the registered entity's COP but prior to the creation of the Audit Notification Letter. There is an opportunity to enhance existing communication processes, such as Audit Notification Letter and Compliance Audit report, by providing an explanation for the inclusion of Reliability Standards not listed in the COP. Audit report and ANL templates do not provide guidance on explaining scope determination that reflects emerging risks and priorities.	While entities must be compliant with all applicable Standards and Requirements at all times, and RF may monitor compliance for all applicable Standards and Requirements, RF recognizes the value of communication on audit scope, and is transparent with entities about its risk-based monitoring approach and processes. RF has done significant outreach regarding the purpose of the IRA and COP and utilizes the Coordination Presentation for both audits and spot checks for entities to discuss any question they have regarding the audit notification package, which includes the audit scope. Through years of experience, RF has recognized that direct dialogue is the best way to	Regional Entity Director, Compliance Monitoring	Low

Observation #	Location/Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		Without the explanation, not all registered entities or observers may understand how the audit scope resulted from a risk-based approach to compliance monitoring. This lack of understanding can erode confidence in the ERO Enterprise's CMEP activities. In the cases in question, there were practical reasons to have these Reliability Standards included in the scope. Providing a communication vehicle that explains those reasons will help the registered entity and observers understand where COPs and audit scope fit into an agile, proactive monitoring strategy. This improvement will reinforce the COP as a value-added tool that is instructive but not determinative regarding scope.	address these issues, and RF will continue these communication efforts in the future. Regarding management actions needed, ReliabilityFirst will continue its communication methods described above. ReliabilityFirst will also work with the ERO Enterprise on any efforts going forward to create an additional ERO-wide communication vehicle.		

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment E

Appendix 4A Audit Report – SERC Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP Appendix 4A) Audit

SERC Reliability Corporation

May 17, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Jason Blake, President and CEO

From: NERC Internal Audit

Date: May 17, 2022

Subject: CMEP 4A Audit - SERC

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity (RE) Compliance Monitoring and Enforcement Program (CMEP 4A) Audit.

The audit objective was to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and delegation agreements.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Manny Cancel, NERC
Lonni Dieck, SERC (Board)
Kelly Hanson, NERC
Holly Hawkins, SERC
Todd Hillman, SERC (Board)
Mark Lauby, NERC
Sonia Mendonca, NERC
Jim Robb, NERC
Janet Sena, NERC
Brian Thumm, SERC

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

SERC Reliability Corporation (SERC)
CMEP Appendix 4A Audit

Background

The **SERC Reliability Corporation** (**SERC**), is located in Charlotte, NC and is responsible for the reliability and security of the electric grid across the southeastern and central regions of the United States. This area covers approximately 630,000 square miles and serves a population of more than 91 million. It includes all or portions of Florida, Georgia, Alabama, Mississippi, Louisiana, Texas, Oklahoma, Arkansas, Missouri, Iowa, Illinois, Kentucky, Tennessee, Virginia, North Carolina, and South Carolina. SERC's footprint includes approximately 267 registered entities.

The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Program, which is required at least once every five years.

Effective as of 2019, the RAM and Enforcement departments completed two separate and significant process improvement projects to improve SERC's timely resolution and mitigation of noncompliance. The groups collaborated on scope of the violations, risks, and root causes to determine required mitigation activities to remediate violations and prevent reoccurrence. In 2021, SERC's initiatives drove marked programmatic improvements. SERC processed 402 violations, a 24% reduction of violations from 2020, reducing the total inventory to 304 violations by the end of the year, and reducing the average age of inventory from 13.7 months to 10.7 months.

The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The audit objective is to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreements.

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of risk based CMEP, including the utilization of monitoring tools as defined within the ROP, or directed by NERC.

SERC improved processes over the last year which led to efficiencies throughout their CMEP program. For example, SERC restructured their CMEP department in September 2021, by creating a Risk Awareness and Oversight (RAO) department to focus efforts on Inherent Risk Assessment (IRA), Entity Risk Profile (ERP), and Compliance Oversight Plans (COPs), and to ensure SERC is deploying its internal resources effectively to reduce risk to the BPS. SERC's Risk Assessment and Mitigation (RAM) department took the initiative to provide a mentor program for new RAM hires, by

shadowing a senior staff member until a probationary period ends, at which time the staff can complete work on their own, as a means of solidifying process and responsibilities. SERC has prioritized focus on Facility Ratings, as demonstrated by performing outreach, lessons learned, and virtual presentations to stakeholders across the ERO Enterprise. In addition, SERC's Data Analytics department provides dashboards which report trends and status of critical components of CMEP activities, such facility ratings, GADS/TADS/MIDAS performance, and others. This effort showcases SERC's diligence to use data as a tool for CMEP. Lastly, efficiencies were evident through improved coordination between RAM and Enforcement review of potential noncompliance, streamlining the process by eliminating backlog and aged issues.

During the course of the audit, we identified themes related to inconsistent process execution. For example, there were inconsistencies in the development of Inherent Risk Assessment (IRA), Entity Risk Profiles (ERP), and Compliance Oversight Plans (COPS); SERC's internal oversight of training and learning program objectives for CMEP staff; monitoring of industry subject matter experts conflict of interest disclosure; and SERC's evaluation of Registered Entity internal controls during registered entity audit pre-planning and planning activities. In addition, newly hired CIP auditors had a lengthy delay in completing the required NERC auditor training. These inconsistencies may negatively impact risk-based audit scoping, as well as auditor preparedness respectively.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
- Compliance Oversight Plans (COPs)
  - Entity Risk Profile (ERP)
  - Internal Controls
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits, Spot Checks, Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	3	0	3
Risk Assessment	0	0	0	0
COPs	0	2	0	2
Enforcement	0	0	0	0
Monitoring Tools	0	0	0	0
Supporting Activities	0	0	0	0
Total	**0**	**5**	**0**	**5**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	CMEP staff auditor training was not monitored for timely completion	Associates may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties.
Medium	Training and learning program process documentation for CMEP staff is not formalized	Staff is not effectively executing responsibilities of the role and building capabilities to grow and develop skills in critical program areas. Gaps in training of staff and ensuring adherence to training policy can lead to ineffective execution of expected performance.
Medium	COI process was not consistently applied to Industry Subject Matter Experts	Conflicts of Interest (COI) are not detected and result in undue influence over or bias over CMEP activities.
Medium	IRA-ERP-COP Inconsistencies in Peer Review	Inadequate risk oversight of the registered entities.
Medium	Evaluations of Internal Controls lacked consistency	Lack of registered entity understanding of internal controls, and lack of internal controls procedures, undermines a risk-based approach to compliance and reliability.

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
1.	**Governance: Training**	**CMEP staff auditor training was not monitored for timely completion** Auditors must complete all NERC or NERC-approved Regional Entity auditor training applicable to the Compliance Audit, per Section 3.1.5.2 of the ROP ('Foundations of Auditing' and 'Gather Quality Evidence'). Our audit identified two of three new auditors hired during the audit period that did not complete the required training timely • 21 weeks to complete training for one individual • One course remained incomplete after 14 weeks for another individual In addition, one of those new hire served on an audit team as an observer prior to completing the training per NERC procedure. Without ensuring staff completes required auditor training in a timely manner, and in conjunction with the requirements for an observer role, the individual may not be adequately prepared to execute procedures with the required knowledge or competencies. Management should ensure training is provided timely and consistent within NERC requirements for all CMEP new hires.	SERC agrees with the NERC observation that there are process improvements needed to ensure that CMEP staff auditor training is provided in a timely and consistent manner, within NERC requirements for all new hires. SERC commits to the following actions: Review and enhance processes to improve controls to validate that new hires are assigned the appropriate training and that the training is completed in the appropriate timeframe, including prior to assigning them as a member of an audit team Evaluate whether a dedicated, centralized resource is more effective and efficient than relying on separate department managers to implement the same process. This dedicated role could have the responsibility of assigning and validating	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity, Manager, Outreach & Training	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
			timely completion of all required CMEP training for new hires Whether centralized or decentralized, training program oversight will be responsible for escalating issues to management, and to maintain accurate tracking/records of all required CMEP staff training Update applicable guidance documents to reflect the method chosen for providing additional oversight to CMEP staff auditor training requirements Update audit planning process documentation to include a step that validates all audit team members have completed the required training prior to being assigned to an audit team			

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
2.	**Governance: Training**	**Training and learning program process documentation for CMEP staff is not formalized** CMEP staff should be trained on processes and tools related to their area of responsibility. SERC does not maintain formal training process documentation within each CMEP department, or in a centralized location. Without training and learning program documentation, personnel may not receive the guidance to perform their CMEP responsibilities. CMEP department's training and learning programs should include the development of formal training and learning process documentation, and the tracking of employee progress.	SERC agrees with the NERC observation that there are opportunities for improvement in documentation of training program processes. SERC commits to the following actions: Develop and maintain process documentation for a CMEP training program that includes a tracking mechanism to validate individual employee progress As noted for Observation #1, evaluate whether a dedicated, centralized resource is more effective and efficient than relying on separate department managers to implement the same process. Update applicable guidance documents to reflect the method chosen for enhancing training and learning program process documentation for CMEP staff	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity Manager, Outreach & Training	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
3.	**Governance: Conflict of Interest (COI)**	**COI process was not consistently applied to Industry Subject Matter Experts** SERC's COI and Business Ethics Policy for SERC Representatives requires that industry subject matter experts (ISMEs) disclose any COI from the time they are placed on an audit team until their involvement with the audit has completed. Of the two ISMEs assisting during the audit period, SERC was unable to provide a current COI for one individual. An actual or potential conflict of interest can increase the risk of bias and/or undue influence. SERC must ensure each ISME submits COI disclosure during the time they participate on audits in adherence to the COI and Business Ethics Policy. The policy should be updated to reflect any additional controls put in place.	SERC agrees with the NERC observation that there are opportunities for improvement to the process related to collecting and validating ISME COIs. SERC commits to the following actions: Review and enhance processes to improve controls to validate that an ISME completes a COI form prior to participating in each audit engagement they are assigned. Ensure audit planning process documentation includes a step that ensures validation that all audit team member requirements are met before participating in any engagement, including the completion of a COI form Reevaluate the protocols and safeguards surrounding ISME participation in audit engagements to ensure that such engagements do not create any appearance of a conflict of interest	November 30, 2022	Regional Entity VP, General Counsel & Corporate Secretary Regional Entity Director of Reliability Assurance	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
4.	**Compliance Oversight Plans: IRA-ERP-COP**	**IRA-ERP-COP Inconsistencies in Peer Review** The Inherent Risk Assessment, Entity Risk Profile, Compliance Oversight Plan (IRA-ERP-COP) procedure during the audit period required peer review of IRA-ERPs. A representative sample of registered entities selected within the audit period, noted the following: • 1 registered entity did not include evidence of peer review, an ERP, or a COP report • 1 ERP provided was not completed in its entirety (CMEP Implementation Plan Comparison table was not completed to demonstrate rationale for not including standards in the monitoring recommendation) The benefit of performing a peer review of IRA-ERPs is to maintain quality standards and improve performance. Without strengthening the review process, there may be inadequate risk oversight of the registered entities. SERC should ensure that there is a thorough review process in place for IRA-ERP-COPs to include determination that ERPs are filled out completely, and that each registered entity has all applicable documents reviewed and finalized. The integrity of the review process is	SERC agrees with the NERC observation that there are opportunities for improvement to the IRA-ERP-COP process to ensure consistent execution. SERC feels confident that the Risk Awareness and Oversight department that was formed in September 2021 to provide increased focus on IRA-ERP-COPs will address this observation. As SERC continues to develop the Risk Awareness and Oversight team, it commits to the following actions: Review and enhance process documentation to provide clarity on peer review expectations and validation of completeness. Ensure process documentation clearly states roles and responsibilities, preserves the objectivity and independence of the Risk Awareness and Oversight team's decision making	November 30, 2022	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Senior Manager, Risk Awareness & Oversight	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		paramount to detect and correct errors or omissions.	capability, and highlights the steps required to validate the completeness of records			
5.	**Compliance Oversight Plans: Internal controls**	**Evaluations of Internal Controls lacked consistency** Internal controls serve to minimize overall risk for failure of compliance. The Rules of Procedure and the NERC ERO Enterprise Guide for Internal Controls state that there should be a clear approach or procedure in which the Regional Entity evaluates the internal controls of a registered entity. SERC Registered Entities have varying levels of maturity with respect to Internal Controls. This was acknowledged during interviews with SERC staff, and evidenced by a registered entity sampled who was unable to respond to an internal control request for information as part of audit preplanning. SERC requested the entity develop an internal control program; however, there was no evidence of follow up or guidance/training, suggesting a lack of consistency in engaging with entities about their internal controls programs. This may result in unclear communication from SERC as to what the expectation is of a registered entity, as well as the required responses to internal control requests.	SERC agrees with the NERC observation that its program for assessing Registered Entity Internal Controls would benefit from additional consistency and documentation. SERC agrees that an enhanced approach to working with specific entities can help inform risk-based decisions about the sustainability of the individual entity's compliance program. This would also enhance the consistency of SERC's outreach in this space. SERC commits to the following actions: Evaluate potential programmatic changes, which will include the following elements: ○ identify entities with weak or no internal controls, to help SERC	February 1, 2023	Regional Entity VP, Performance Improvement & Risk Management Regional Entity Director of Reliability Assurance Regional Entity, Senior Program Manager, Strategic Initiatives & Continuous Improvement	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		Without the consistent application of a process to review registered entity responses or questions related to internal controls, the effectiveness of the registered entity's mitigation of risk, and the opportunity to provide feedback on potential control weaknesses that may lead to non-compliance is limited. Internal controls are fundamental to a risk-based approach to ensuring reliability. Therefore, SERC should identify entities with weak or no internal controls and develop guidance or an approach to assist. This practice should exist outside the audit schedule to encourage registered entities to maintain and implement internal controls to increase the effectiveness of risk-based CMEP in ensuring reliability.	develop guidance or specific approaches for specific entities ○ increase specific awareness about internal controls deficiencies broadly across the Region and narrowly with specific entities ○ guide entities toward making appropriate decisions about the implementation of an internal controls program Evaluate opportunities to ensure consistent application of its process, and incorporate any changes necessary, as appropriate			

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment F

Appendix 4A Audit Report – Texas Reliability Entity

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

Texas Reliability Entity, Inc. (Texas RE)

Date: August 31, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Jim Albright, President and CEO

From: NERC Internal Audit

Date: August 31, 2022

Subject: CMEP 4A Audit – Texas RE

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity (RE) Compliance Monitoring and Enforcement Program (CMEP 4A) Audit.

The audit objective was to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and delegation agreements.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Jim Albright (Texas RE)
Manny Cancel (NERC)
Curtis Crews (Texas RE)
Derrick Davis (Texas RE)
Kelly Hanson (NERC)
Jeff Hargis (Texas RE)
Mark Lauby (NERC)
Sonia Mendonca (NERC)
Jim Robb (NERC)
Janet Sena (NERC)
Joseph P. Younger (Texas RE)

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

Texas RE
CMEP Appendix 4A Audit

Background

The **Texas RE**, is a Texas 501(c) (3) non-profit corporation that is the Regional Entity for the area of Texas served by the Electric Reliability Council of Texas (ERCOT). Through a Delegation Agreement with the North American Electric Reliability Corporation (NERC), which is approved by the Federal Energy Regulatory Commission (FERC), Texas RE is authorized to develop, monitor, assess, and enforce compliance with NERC Reliability Standards, develop regional standards, and assess and periodically report on the reliability and adequacy of the bulk power system in the ERCOT region. Texas RE is independent of all users, owners, and operators of the BPS.

There are approximately 293 registered entities in Texas RE's footprint. The membership sectors are: System Coordination and Planning, Transmission and Distribution, Cooperative Utility, Municipal Utility, Generation, and Load-Serving and Marketing.

Texas RE provides a robust program to oversee and ensure reliability of the ERCOT Interconnection, which covers approximately 75 percent of Texas' land area and 90 percent of its electricity load. The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Program, which is required at least once every five years.

Texas RE has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The audit objective is to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreement.

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of risk-based CMEP, including the use of monitoring tools as defined within the ROP, or directed by NERC.

Throughout the audit, Texas RE staff were both accommodating and responsive to requests from IA, and their diligence and professionalism were appreciated.

Noteworthy remarks to Texas RE's CMEP program are as follows:

- Texas RE CMEP Engage tool is a comprehensive in-house software platform tool that serves well for maintaining IRA, COP, performance considerations, and other CMEP monitoring activities.
- Texas RE thoroughly tracks CMEP staff training and education.
- The multi-year audit schedule is a holistic resource for tracking audit and self-certification activity across the RE footprint. The tracker captures scheduling from 2006 to 2030, and includes each entity's registered functions, NERC ID (i.e. NERC Compliance Registry #), MRRE LRE/ARE designation, and COP monitoring interval.

During the course of the audit, we identified themes related to inconsistent process execution. For example, we noted the exclusion of applicable NERC CMEP IP risk elements into compliance oversight plans and audit scoping; a deviation from the COP procedure; and long-term compliance monitoring intervals for some lower-risk registered entities.

The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment
  - Regional Risk Assessment
  - Potential Non-Compliance (PNC)
  - Mitigating activities
- Compliance Oversight Plans (COPs)
  - Entity Risk Profile (ERP)
  - Internal Controls
- Enforcement activities and actions
  - Issue processing
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits, Spot Checks, Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)
- Supporting Activities
  - Methodologies and Processes
  - CMEP IP, Annual ERO Oversight Plan
  - Physical Security

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	0	0	0
Risk Assessment	0	1	0	1
COPs	0	1	0	1
Enforcement	0	0	0	0
Monitoring Tools	0	0	1	1
Supporting Activities	0	0	0	0
Total	**0**	**2**	**1**	**3**

High/Medium/Low-Risk Rated Observations *(High, medium, and low risk observations require a management action plan)*		
Rating	**Observation**	**Risk**
Medium	Exclusion of relevant CMEP IP Risk Element Standards and Requirements from Entities' Compliance Oversight Plans was not justified or supported through documented rationale	Excluding NERC CMEP IP Risk Element Standards and Requirements from an applicable entity's COP results in reduced or incomplete monitoring; potential for risks to be unmitigated and/or lead to non-compliance, adversely impacting reliability and security.
Medium	Adherence to local policy for development of COPs is not followed.	An oversight strategy is not defined, along with the appropriate monitoring tools and interval to manage risk.
Low	Compliance monitoring category levels for lower risk entities in COPs did not reconcile to the audit schedule prepared by Texas RE. Several entities with category 5 designations were scheduled for 8-year intervals.	Inconsistent application of the ERO Enterprise Oversight strategy and lack of support or rationale for changes reduce the effectiveness of CMEP in ensuring reliability and security across all entities within its footprint in a risk-based manner.

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
1.	**Risk Assessment Rules of Procedure; Section 400.401.6 Risk Elements**	**Exclusion of relevant CMEP IP Risk Element Standards and Requirements from Entities' Compliance Oversight Plans was not justified or supported through documented rationale** Review of the COPs created in the audit period against the CMEP IP Risk Elements applicable standard and requirements identified that multiple COPs exclude standards and requirements that should apply to the entity. • Five entities had a total of 34 applicable Standards and Requirements excluded with no clear action for monitoring or oversight plan. As noted in the "Conducting Inherent Risk Assessments" DESK 10.18, the COP is used to "create a scope for an upcoming engagement, Risk Staff will consult the COP for the list of Requirements selected for active oversight". In addition, the "COP process uses this information to create a COP consisting of all Requirements applicable to the entity, the monitoring methods available for oversight, and the monitoring interval for the entity". The CMEP IP 2020 states that "notably, the implementation plan is not intended to be a representation of just "important" Reliability Standards requirements; rather, it is intended to reflect the ERO	Texas RE appreciates the auditors' observation regarding the opportunity to enhance Texas RE's policies and procedures for documenting its review of, inclusion or exclusion, and proposed monitoring for CMEP IP Risk Elements. To address this observation, Texas RE will adopt process enhancements to improve Texas RE's documented justifications when it elects to exclude the Requirements associated with applicable Risk Elements from Appendix B of the registered entity's COP.	October 31, 2022	Regional Entity Director, O&P Compliance and Risk Assessment Regional Entity Manager, Risk Assessment	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		Enterprise's prioritization within its CMEP based on its inputs and to communicate to registered entities to bring collective focus within their operations to address each prioritized risk". This illustrates the importance of the risk element standards being prioritized, monitored, and included for oversight action. There are no procedures or protocols to ensure that the identified NERC CMEP IP Risk Elements for the year are included in the COP for the applicable entity. Failure to review or properly assess NERC CMEP IP Risk Elements and their applicability to a registered entity's compliance oversight could result in detecting risks and threats to the bulk power supply system. Either create or include in policy and procedures documentation of a direct review of NERC CMEP IP Risk Elements, how they are assessed and then included or excluded, and their monitoring for applicable entities.				
2.	**Compliance Oversight Plan (COPS)** **ROP RE Risk-based compliance**	**Adherence to local policy for COP development is not followed** Development and refreshing of COPs based on other significant performance considerations and monitoring activities	Although Texas RE believes the entity in question has elements of a COP in place, Texas RE acknowledges the audit team's observation regarding the importance of timely development and	December 31, 2022	Regional Entity Director, O&P Compliance and Risk Assessment	Medium

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
	oversight 403.10	doesn't necessarily lead to development of refreshing of a COP. A COP was not developed for a registered entity that experienced significant performance considerations from the period of 2018 to present. • Two anonymous complaints were filed in 2019 • Physical Security Event in 2019 • Unannounced audit in 2020 Texas RE's 'Developing Compliance Oversight Plans Procedure' states Texas RE develops a COP for every Registered Entity in its region, and staff stated a COP will be developed for each newly registered entity within six months. Triggers may result in refreshing a COP, such as a change in one or more performance considerations impacting the risk category and subsequently the oversight strategy. Texas RE provided a 2018 IRA Summary Report, and Internal Work Papers (2021 IRA Risk Factor Analysis, and Risk Performance Data spreadsheet) to the audit team. A COP serves both internal and external parties, and Texas RE was not able to provide evidence of articulating the oversight strategy to the entity since 2018, although performance considerations changed.	updating entity COPs as conditions warrant and per our internal COP procedure. Texas RE is in the process of implementing a risk-based schedule for revising COPs to use the current ERO COP template, and that risk-based schedule anticipates that in 2022 Texas RE will refresh the COP for the registered entity at issue to reflect the most current facts and circumstances in advance of the registered entity's next scheduled compliance engagement. To address the observation more generally, Texas RE will adopt process improvements to include creating or refreshing a COP using the most current ERO COP template in advance of future unscheduled Compliance Audits.		Regional Entity Manager, Risk Assessment	

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		While Texas RE's COP interval scheduler indicated a COP would be developed in 2020, the target date was moved to end of 2022 ahead of the 2023 guided self-certification. The current oversight strategy may not accurately represent a risk-based approach, or designating the proper monitoring tools and intervals without a relevant COP based on consideration of multiple performance considerations (i.e. Culture of Compliance events). Risk management should ensure that IRAs and COPs are developed according to internal procedures, leveraging the most current ERO Enterprise guidance, tools and templates.				
3.	**Compliance Monitoring Rules of Procedure; Section 400.3.1 Compliance Audits**	**Compliance Monitoring Intervals for Low-Risk Registered Entities** Six of seven lower-risk registered entities sampled were designated as Category 5 in their respective COPs, yet Texas RE's audit schedule tracker indicates 8-year monitoring intervals, with no compliance monitoring tools utilized in the interim. The NERC Compliance Oversight Plan Process Enhancements guidance (November 13, 2020), includes for the oversight strategy, that Category 5, lower inherent risk without demonstrated positive performance should be monitored	Texas RE appreciates the audit team's observation. To address the audit team's recommendations, Texas RE will review other Regional Entities' processes for capturing periodic changes to entity inherent risk, as well as demonstrated positive performance. Based on this review, Texas RE will consider process improvements that are a fit for the Texas RE footprint's unique characteristics, including Texas RE's access	October 31, 2022	Regional Entity Director, O&P Compliance and Risk Assessment Regional Entity Manager, Risk Assessment	Low

Observation #	Location	Observation	Management Action Plan (MAP)	Action Plan Due Date	Responsible Person(s)	Impact
		between 5-7 years. Category 6, lower inherent risk with demonstrated positive performance at 6+ years. To extend compliance monitoring of registered entities beyond 7 years without intermittent monitoring can increase risk to reliability and security. In addition, COP monitoring categories should reflect the appropriate monitoring interval, along with associated department tracking mechanisms. Texas RE should monitor lower-risk entities in between long interval engagements by capturing evidence of demonstrated positive performance on Reliability Standards that are applicable to the entity. An example would be an annual risk questionnaire to all registered entities, with responses due and appropriate follow up and monitoring, in line with a risk-based monitoring approach. In addition, Texas RE should ensure that it develops clear, documented justifications if monitoring intervals are extended for lower-risk entities.	to real-time performance data within the Texas Interconnection that may obviate the need to request certain performance information and data directly from registered entities via a questionnaire. In addition, Texas RE will adopt process improvements to ensure that Texas RE develops clear, documented justifications if monitoring intervals are extended for lower-risk entities. These process improvements will include a periodic reassessment of the justification during the period between compliance engagements in situations in which Texas RE has elected to extend entity intervals, including a reassessment of the entity's overall Compliance Oversight Plan			

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment G

Appendix 4A Audit Report – Western Energy Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FINAL REPORT

Regional Entity Compliance Monitoring and Enforcement Program (CMEP 4A) Audit

Western Electricity Coordinating Council (WECC)

Date: August 4, 2022

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

To: Melanie Frye, President and Chief Executive Officer
Jillian Lessner, Chief Administrative and Financial Officer

From: NERC Internal Audit

Date: August 4, 2022

Subject: Regional Entity CMEP 4A Audit – Western Electricity Coordinating Council (WECC)

****

Enclosed, please find Internal Audit's report as it relates to the Regional Entity (RE) Compliance Monitoring and Enforcement Program (CMEP Appendix 4A) Audit.

The audit objective is to assess the RE's implementation of the NERC CMEP and determine whether the program effectively meets the requirements under the Rules of Procedure (ROP) Section 400, Appendix 4C, and the corresponding annual CMEP Implementation Plan (IP), including monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreements.

Should you have any questions about this review, please contact Kristin Miller at kristin.miller@nerc.net or at 404-230-4663.

CC: Chris Albrecht (WECC)
Scott Brooksby (WECC)
Manny Cancel (NERC)
Michael Dalebout (WECC)
Kelly Hanson (NERC)
Kim Israelsson (WECC)
Mark Lauby (NERC)
Sonia Mendonca (NERC)
Deborah McEndaffer (WECC)
Steven Noess (WECC)
Jim Robb (NERC)
Janet Sena (NERC)

Note: Individuals whose names appear in bold type are management action plan owner(s).

EXECUTIVE SUMMARY

Western Electricity Coordinating Council (WECC)
CMEP Appendix 4A Audit

Background

The **Western Electricity Coordinating Council** (**WECC**) is one of six REs subject to the Electric Reliability Organization's oversight authority under a delegation agreement. Of those six entities, WECC oversees the largest and most geographically diverse region, known as the Western Interconnection. WECC works with entities across the West to further the common theme of grid reliability. Through its various reliability-related activities, WECC provides critical support to the Reliability Coordinator and the resource owners/operators throughout the Western Interconnection. One of WECC's functions is coordinating high voltage intertie paths throughout the region.

WECC's Headquarters are located in Salt Lake City, Utah. WECC's footprint extends from Canada to Mexico and includes the provinces of Alberta and British Columbia, the northern portion of Baja California, Mexico, and all or portions of the 14 Western states between. Additionally, WECC's footprint includes approximately 436 registered entities consisting of municipal utilities, cooperatives, investor-owned utilities, federal power marketing agencies, Canadian Crown Corporations, and independent power producers. Lastly, the WECC CMEP aligns structurally within the Reliability and Security Oversight function and employs approximately 68 professionals encompassing Entity Risk Assessment and Registration (ERAR), Entity Monitoring, Program Analysis and Administration, and Enforcement and Mitigation.

The NERC Regional Entity audit program was established to assess the Regional Entity's implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) and determine whether the program, as implemented by the Regional Entity, effectively meets the requirements under the CMEP, the NERC Rules of Procedure (ROP), and the corresponding annual Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP). Each year, NERC identifies risks to focus CMEP activities through its annual CMEP IP.

NERC Internal Audit independently performed the audit of the Regional Entity Compliance Program, which is required at least once every five years.

WECC has participated in periodic self-certifications related to its CMEP and activities up to the period of this engagement. The audit report contains observations and recommendations to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS).

Audit Summary

The audit objective was to assess the RE's implementation of the NERC CMEP and determine whether the program, as implemented by the RE, effectively meets the requirements under the CMEP, the ROP, and the corresponding annual CMEP Implementation Plan (IP), including RE monitoring and enforcement of compliance with relevant Reliability Standard requirements, and the delegation agreements.

The scope of the audit engagement included select areas of the ROP, Appendix 4C, annual CMEP IP risk elements and associated areas of focus and monitoring schedules, and an evaluation of the Regional Entity's approach to and application of risk based CMEP, including the utilization of monitoring tools as defined within the ROP, or directed by NERC.

Overall, WECC's CMEP was representative of a risk-based approach and included numerous investments and innovations to connect processes and data to enable data driven decisions. This was illustrated by end to end risk assessment processes to Compliance Oversight Plans (COPs), developed for the majority (97%) of registered entities within the WECC footprint. A disciplined approach is applied to determine and continuously monitor registered entities with the appropriate oversight strategy, tool(s) and intervals, influenced by critical inputs (i.e. "triggers") evaluated with periodicity based on registration changes, analysis, performance considerations and risk.

The most commonly executed monitoring tools are: Compliance Audits (both CIP and Operations and Planning), Self-Certifications and Self-Reporting. Throughout the period of our audit (2020-2021), 42 audits were performed and 450 Self – Certifications. Spot Checks are performed minimally, and participation by registered entities within the Self-Logging program is at a nominal 2% of the total footprint.

In conclusion, the WECC risk-based approach to CMEP is effective and locally developed tools provide the required efficiencies to manage oversight for the largest, geographically diverse region with climate, social and energy challenges. However, WECC recently experienced turnover in three key CMEP management roles, such as, Director of Enforcement and Mitigation, Director of ERAR, and Supervisor, Internal Controls. These vacancies may impact the sustainability of processes and effectiveness of CMEP oversight in the short term. Lastly, there are opportunities to continue to improve processes and controls related to Complaints/Investigations, Training, and overall systematic recordkeeping of key data within local tools (IRAs/COPs/internal controls…) as the transition to Align is completed by year end 2022.

Audit Period and Scope

The period under review was January 1, 2020 through December 31, 2021.

The scope included the following:

- Governance/Regional Delegation Agreements (RDA)
  - Compliance Registry - CMEP Contacts
  - Conflict of Interest (Board and Employees)
  - Training
  - Complaints and Investigations
- Risk Assessment/Risk Categories/Factors/Elements
  - Inherent Risk Assessment (IRA)
  - Regional Risk Assessment
  - Mitigating activities
- Compliance Oversight Plans (COPs)
  - Internal Controls
- Enforcement activities and actions
  - Issue processing/potential non-compliance
  - Disposition determination
  - Penalty processes/assessments
- Compliance Monitoring Processes and Tools
  - Compliance Audits
  - Spot Checks
  - Self-Reports, Self-Logging, Self-Certifications
  - Periodic Data Submittals (PDS)

Observation Summary

	Ratings			
Area	**High**	**Medium**	**Low**	**Total**
Governance	0	0	1	1
Risk Assessment	0	0	0	0
COPs	0	1	0	1
Enforcement	0	1	0	1
Monitoring Tools	0	1	0	1

• Supporting Activities ○ Methodologies and Processes ○ CMEP IP, Annual ERO Oversight Plan ○ Physical Security	Supporting Activities	0	0	0	1
	Total	**0**	**3**	**1**	**4**

High/Medium/Low-Risk Rated Observations
(High, medium, and low risk observations require a management action plan)

Rating	Observation	Risk
Low	Methods or tools to ensure training tracking and monitoring is not consistent, and training or learning program process or procedure documents were not developed or updated within a stated frequency.	Staff may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties.
Medium	Potential Non-Compliances (PNCs) identified through Self-Certifications performed in 2020, have not yet been recorded into Align and subsequently reported to NERC and FERC in accordance with the RDA and ROP.	Delays in performing Preliminary Screens in accordance with RDA Section 6b/c/d; ROP 3.0, 3A.1, and 3.8; the risk remains unmitigated impacting reliability and security.
Medium	Changes in IRA and COP processes revealed that registered entities within an assigned monitoring interval did not have an updated COP prior to or after a Compliance Audit, and several did not contain a review of internal controls.	Inconsistent IRA and COP processes reduce the risk-based application regional monitoring and does not adequately address reliability and security risk against the required monitoring interval.
Medium	Review and disposition of anonymous complaints were not managed timely, and were prematurely or inaccurately closed due to insufficient information.	An essential component of an ERO compliance program is not effective for addressing alleged violations of Reliability Standards or deficiencies in internal controls that adversely impact reliability and security.

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
1.	**Governance: Training** **NERC ROP 402 – NERC Oversight of RE CMEP** **402.9 – Auditor Training**	**Enhance processes to ensure CMEP staff receive the appropriate training and learning programs timely** CMEP staff are required to be trained on processes and tools related to their area of responsibility. The WECC Entity Monitoring team identifies, applies and tracks required training in an ad hoc or inconsistent manner. Training applicable or required is not formally evidenced, as some certificates were issued while other attestations occurred. CMEP staff may not be equipped to provide the subject matter expertise or demonstrate the responsibilities necessary to consistently and accurately perform CMEP duties. Training process documentation, including requirements to provide training and track completion by applicable departments (functional and/or Human Resources) should be established.	For all remaining 2022 audit engagements (QTR 3 & 4), we will review and confirm Audit Team Lead (ATL) training records are accounted for and archived for individuals assigned as ATLs by **August 1, 2022**. We will update our Personnel Tracking Sheet to reconcile dates of completed training and ensure evidence of training is archived and available (e.g., certificates of completion). In addition to various information tracked in this sheet, we track the dates of completing NERC Foundations of Auditing and Gathering Quality Evidence courses; the sheet will be updated to capture dates of completing the NERC ATL training by **September 1, 2022**. If gaps are found, we will task the individual to promptly complete the requisite training by **September 1, 2022.** We will document a process for quarterly review of training records. We will implement the process beginning in quarter four of 2022. The process will identify roles, responsibilities, and controls, used to ensure quarterly reviews are in place by **October 1, 2022.** As part of the annual audit scheduling process, we will outline detailed steps to verify ATL training records are checked prior to finalizing ATL assignments each year. The process will identify roles, responsibilities, and controls, used to ensure training records are verified and accounted for. This process will be implemented with the 2024 scheduling (which will take place by **March 31, 2023**), and any necessary adjustments for 2023, such	Regional Entity Manager, Program Analysis and Administration	Low

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
			as changing ATL assignments and be in place by **November 1, 2022.** The Operations Lead for Entity Monitoring partners with the Audit Team Managers to plan how and when new members are added to audit engagements. As part of the on-boarding process, any new team members and/or observers will be required to complete the required training (NERC Foundations of Auditing and Gathering Quality Evidence) prior to finalizing the engagement roster.		
2.	**Compliance Monitoring: Self-Assessments/ Preliminary Screen** **RDA Section 6 ROP Appendix 4C – 3.0 Compliance Monitoring; 3.2/3.2.1 Self-certifications/ Process Steps; 3.8 Preliminary Screen**	**Identify, Assess and Record Potential Non-Compliance (PNC) timely by performing Preliminary Screen and Determining Disposition** A review of Guided Self-Certifications performed during the period under audit revealed two instances where PNCs were identified during the self-certification by the registered entities or WECC, however, not recorded within system of record (WEBCDMS or Align) for evaluation and disposition as of June 2022. If a compliance monitoring process reveals a potential non-compliance with a Reliability Standard, the RE will conduct a Preliminary Screen of the potential non-compliance in accordance with ROP Appendix 4C, Section 3.8 (Preliminary Screen). Delays in processing potential non-compliance may allow violations of Reliability Standards to go unmitigated and adversely impact reliability and security of the BPS.	Entity Monitoring staff has notified the two Registered Entities of the PNC identified during the Guided Self-Certification on 07/15/2022 and 07/18/2022 respectively. After verbal notification, a closure letter was sent to each Registered Entity on 07/19/2022 to notify them the GSC is closed. A PNC will be entered into Align no later than **07/22/2022**. Review of GSC evidence of a third Registered Entity with the Entity; prompted a change in their GSC status from Compliant to Not Compliant. Entity Monitoring also identified an Area of Concern for another Requirement. A GSC closure letter was sent to the Registered Entity on **07/19/2022** with the AOC. In addition, we have developed a procedure providing guidance to the Entity Monitoring team around roles and responsibilities for Self-Certifications, including steps in review of Registered Entity submittal, how to address potential non-compliance and closure of the engagement. WECC's procedures now ensure potential noncompliance are	Regional Entity Director of Entity Monitoring	Medium

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		The Entity Monitoring team did not report the potential non-compliance identified in the self-certifications as documentation revealed pending communication with the affected registered entities. The lack of entry into the CMEP system may have caused an inadvertent omission or oversight to process the potential compliance timely. WECC should ensure that potential non-compliance identified through compliance monitoring processes adheres to Appendix 4C Section 3.0 and 3.8 and are recorded systematically to facilitate timely Preliminary Screens and overall disposition and/or required mitigation.	entered into the system of record and a preliminary screen is performed. Additionally, Reliability and Oversight management has implemented a tracked metric with the goal of completing Self-Certification reviews within 90 days of the due date (or submit date, if later).		
3.	**Risk Assessment/ Compliance Monitoring/ Risk based CMEP: IRAs/COPs** **The Electric Reliability Organization (ERO) Enterprise Guide for Risk-based Compliance Monitoring**	**Develop and Refresh Inherent Risk Assessments and Compliance Oversight Plans within a Standard Periodicity to Support Consistent Oversight Strategy** An IA review of a representative sample of IRA and COPs, with a mix of risk category ratings of 1 through 6 revealed the following: • Discrepancy of risk category with one 3-year audit entity, noted audit interval was Category 1, to be audited every 1-3 years, however, planning tool indicated 2-4 years. IRA and COP refreshed in 2020. The entity was due for an audit in 2021. However, the entity was selected for a FERC audit in 2021, but this was not recorded in WECC's planning tools.	**Modify Entity Risk Profile Tool** • Add validation of final risk category with actual audit timing by **November 15, 2022**. • Review and assess Internal Controls evaluations as part of the ERPT process by November 15, 2022. **Add items to Quality Control Checklist** • Add step to transfer the final audit/COP timing from the ERPT to the IRA_COP Tracker by **August 30, 2022.** **Add items and process change in IRA_COP Milestones and Assignments Tracker** • Add process step to validate audit/monitoring interval when setting next planned refresh by **August 30, 2022.**	Regional Entity Director, Entity Risk Assessment & Registration	Medium

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
	Compliance Oversight Plan Process Enhancements 11/13/2020 **NERC ROP 401 – Scope of the NERC CMEP** **401.6 – Risk Elements**	• Discrepancy of risk category with one 3-year audit entity, noted audit interval should be category 1, however, planning tool indicates 3-5 years. IRA/COP was not refreshed pre or post audit in 2021 and current file indicated IRA/COP from 2018. • Three registered entities did not have IRA/COP updated pre or post audit, and overall it could not be determined what annual CMEP IP focus areas and/or risk elements applied within the monitoring interval and primary CMEP tools. • Internal controls as a performance consideration was not addressed in 80% of COPs reviewed. The Electric Reliability Organization (ERO) Enterprise Guide for Risk-based Compliance Monitoring describes the process used by the Regions to develop entity-specific COPs and serve as a common approach for the North American Electric Reliability Corporation (NERC) and WECC for implementing risk-based compliance monitoring. NERC guidance is that REs should treat the COP as a living document updating it as new, emerging, or unique information is obtained either about the registered entity or about risks to the reliability of the BPS. While feedback from audits is a significant trigger, there are additional triggers for determining if any updates are needed/updating the COP such as changes in registration, a change in the registered entity	**Update WECC Risk Based Monitoring Planner tool** Add audit/monitoring interval to ensure this planning tool is the authoritative source based on ERPT and IRA/COP Tracker input by **September 30, 2022.**		

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		inherent risks (captured in the IRA), new Reliability Standards, changes in controls, emerging risks, changes in performance considerations, FERC scheduled audits, and feedback from CEA staff or other CMEP activities. The discrepancies with risk category and targeted monitoring interval may be due to changes in IRA and COP processes from 2020 to January 1, 2022. For example, tools such as Entity Risk Profile Tool were developed to capture real-time information such as "triggers" and a new IRA/COP combined template was issued by NERC in 2020. Lastly, WECC changed the process to refresh IRA/COP from pre-audit to post-audits in April 2021. Inconsistent processes reduces the effectiveness of the risk based application of the WECC regional monitoring program and reduces the quality and appropriate risk oversight of the registered entity. Align locally developed tools such as the Entity Risk Profile Tool – Entity Ranking, Risk-based Monitoring Planner and IRA/COP Milestones and Assignments Tracker to the ERO Enterprise Guide and Align functionality as applicable. Lastly, ensure established criteria and data within tools and Align substantiate determinations and provide evidence that each registered entity is handled consistently and fairly.			

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
4.	**Governance: Complaints and Investigations** **ROP Appendix 4C – 3.0 Compliance Monitoring Processes** **3.7 Complaints** **3.7.1 Complaints Process Steps** **3.7.2 Anonymous Complainant Notification Procedure**	**Evidence Sufficient Initial Review, Assessment and Final Disposition of Complaints** An anonymous complaint received by WECC during the period under audit revealed that upon forwarding to NERC, the final disposition was not known by the RE as of May 2022. The complaint was sent to RE anonymously by a registered entity employee in May 2021. However, due to a WECC CMEP workflow issue, the complaint was not immediately identified. Subsequently, the complaint was forwarded by WECC to NERC in December 2021. Internal Audit followed up with NERC and learned the complaint was closed due to insufficient information. Evidence to support an initial review and assessment was not provided, only that the complainant could not be reached and NERC's disposition was that the alleged complaint did not violate Reliability Standards. However, the allegations in total warranted a more thorough assessment due to the potential internal control/IT General Control implications related to relevant CIP Standards, and potential initiation of another compliance monitoring or enforcement process. All anonymous Complaints will be reviewed and any resulting compliance monitoring or enforcement processes will be conducted by NERC in accordance with Section 3.7.2 to prevent disclosure identity of the complainant. NERC should fully document the Complaint and the Complaint review, and whether another compliance monitoring process or enforcement process is warranted. If NERC determines that the initiation of another	**WECC CMEP workflow issue** An internal control was added in the WECC Complaint Process dated 5/12/2022 for the Compliance Program Coordinator to test the system monthly and verify no new complaints have been received. A SharePoint alert was set up for the Director of Entity Monitoring and the Vice President of Reliability and Security Oversight to immediately send an email for "All Changes" in the Complaint Forms as a backup to the above internal control. **Prematurely closing Complaints without evidence of initial review and assessment to potentially warrant another compliance monitoring process** For Complaints handled by WECC, language was added to the WECC Complaint Process dated **7/15/22**, for an additional review of the Complaint by the appropriate Entity Monitoring Manager and the Director of Entity Monitoring regarding whether the complaint contains sufficient basis in initiating any applicable Compliance Monitoring process. The Director of Entity Monitoring documents this review, the decision made, and the reasons for that decision. For the May 2021 complaint filed by a registered entity employee, a follow-up to assess all the potential allegations of Reliability Standards will be addressed during the upcoming scheduled audit of the entity during **August 2022**. Specifically, CIP-005-6 R1 and R2 are in scope for the audit for validation of	Regional Entity Director of Entity Monitoring	Medium

Observation #	Location/ Scope Areas	Observation	Management Action Plan (MAP)	Responsible Person	Impact
		compliance monitoring or enforcement process is not warranted, it will notify the Complainant and the RE that no further action will be taken. Prematurely closing Complaints without evidence of initial review and assessment to potentially warrant another compliance monitoring process increases risk of non-compliance or internal control issues impacting reliability and security. In addition, lack of communication with the RE prohibits use of their discretion to incorporate assessment results into further monitoring processes. NERC should perform an initial review and assessment, and document the results thoroughly to support the determination of another compliance monitoring or enforcement process. NERC should assess all the potential allegations within anonymous Complaints to ensure that potential violations of Reliability Standards are addressed with the appropriate monitoring or enforcement activity, and communicated such with the RE in a timely manner.	vendor remote access. In addition, a readiness for check for CIP-005-7 will be conducted, which has the new R3 for vendor-initiated remote access to PACS and EACMS. Based on the rules we observe, risk-based discussions will occur. Recent revisions to the ROP made modifications to Section 4.7.2 of the CMEP to allow Complaints lodged by a person or entity requesting that the complaint's identity not be disclosed to be investigated by NERC or the Regional Entity. This improvement as well as others provides future opportunities to make our processing of Complaints better going forward. The WECC Complaint Process was modified to reflect that for complaints closed without initiating another compliance monitoring process due to insufficient information, we will consider any information received from the compliant during future compliance monitoring activities and to determine whether any other appropriate action should be taken **Lack of communication with the RE in a timely manner** For Complaints handled by NERC, the WECC Complaint Process was modified on **7/15/2022** to include steps to ensure the resolution of all Complaints once submitted to NERC. Beginning July 1, 2022, NERC and WECC will have a quarterly call to discuss progress and resolution of all Complaints.		

Appendix

Audit Approach

The scope of our procedures was determined through our annual risk assessment process, discussions with members of management, and qualitative and quantitative factors identified during the audit-planning phase. The audit engagement team performed various auditing techniques described in the table below:

Technique/Test	Description
Inquiry	Questions and responses to confirm understanding and ownership of processes, risks and controls; potentially establish additional testing criteria.
Inspection	Examining records or documents indicating performance of the control activity or physically examining inventory, systems, books and records.
Observation	Looking at a process or procedure performed by others (e.g., observation of user access reviews by the Company's personnel).
Re-performance	Verifying the operational effectiveness and/or accuracy of a control.
Analytical Procedures	Evaluating information by studying plausible relationships among both financial and nonfinancial data.

Throughout our testing, we used widely accepted audit sampling techniques. These sampling techniques allowed us to obtain audit evidence, which is sufficient and appropriate, and necessary to arrive at a conclusion on the population.

Note: The status of the management action plans will continue to be reported to the Audit/Finance Committee until the observation is successfully remediated.

Observation Ratings

In determining an observation's risk rating (i.e., high, medium, or low), we consider a variety of factors including, but not limited to, the potential impact, the likelihood of the potential impact occurring, risk of fraud occurring, regulatory and legal requirements, repeat observations, pervasiveness, and mitigating controls.