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.