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.