NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

FINAL AUDIT REPORT

NERC Compliance Monitoring and Enforcement Program (CMEP) Audit

Date: January 12, 2023

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, General Counsel and Corporate Secretary
Mechelle Thomas, Vice President and Chief Compliance Officer

From: NERC Internal Audit

Date: January 12, 2023

Subject: NERC CMEP Audit

****

Enclosed, please find Internal Audit's report as it relates to the NERC Compliance Monitoring and Enforcement Program (CMEP) Audit.

The audit objective was to evaluate the effectiveness of the NERC CMEP in achieving its mission, the relationship between NERC and Regional Entity efforts in implementing the CMEP, and the effectiveness of the CMEP.

This report will be posted publicly in accordance with Appendix 4C, as required by ROP Section 406.3 - Independent Audits of the CMEP.

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
Kelly Hanson
Mark Lauby
Nina Jenkins-Johnston
Lonnie Ratliff
Jim Robb
Janet Sena
Teri Stasko

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

EXECUTIVE SUMMARY

NERC Compliance Monitoring and Enforcement Program (CMEP) Audit

Background

Under the NERC Rules of Procedure (ROP), section 400, NERC has developed and implements a Compliance Monitoring and Enforcement Program (CMEP) to promote the reliability of the Bulk Power System by enforcing compliance with approved Reliability Standards in those regions of North America in which NERC and/or a Regional Entity (pursuant to a delegation agreement with NERC or other legal instrument approved by an Applicable Governmental Authority) has been given enforcement authority. Also pursuant to the ROP, NERC oversees each Regional Entity that has been delegated authority to ensure adherence to the rules and terms of the delegation agreement and to ensure consistency and fairness in the execution of the CMEP. Oversight by NERC is accomplished through the development of an annual CMEP review, program audits, and regular evaluations of Regional Entity CMEP performance metrics, risk-based monitoring activities, and performance reports.

In addition, at least every three years, an independent audit of the CMEP is performed under ROP Section 406. The last audit of NERC's CMEP program took place in 2019. The 2022 CMEP audit was executed under the leadership of NERC Internal Audit resources and conducted with observers from the Compliance and Certification Committee (CCC).

Over the past few years, NERC and the Regional Entities have implemented program improvements and have launched a single CMEP information system, Align. Among the improvements to the program are enhancements to tools integral to effective monitoring, such as Inherent Risk Assessments (IRAs) and 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 and the Regional Entities have invested substantial time and effort over the last few years to support the Align implementation, through process harmonization efforts, as well as several training and learning programs.

Align encompasses all aspects of the CMEP and was launched in phases as follows:

- Release 1: Enforcement and Mitigation, and Secure Evidence Locker (SEL)
- Release 2: Self-certification, Periodic Data Submittal (PDS), Attestations, and Technical Feasibility Exceptions (TFEs)
- Release 3: Audits, Spot Checks, and Scheduling Functionality
- Release 4: Enhancements to the Audit and Scheduling Functionality
- Release 4.1: Bug fixes, usability corrections for audit and scheduling functionality
- Release 4.5: Compliance Planning; Inherent Risk Assessment (IRA), and Compliance Oversight Plan (COP)

The audit findings and recommendations have been shared with NERC management and action plans have been developed to address process, control and compliance observations. Further, pursuant to ROP Section 406.3, the final report will be posted by NERC for public viewing in accordance with Appendix 4C after presentation to the NERC Board of Trustees.

Audit Summary

The audit objective was to evaluate the effectiveness of the CMEP in achieving its mission, the relationship between NERC and the Regional Entities in CMEP activities, and the effectiveness of the CMEP in reducing risks to reliability. The audit approach focused on the evaluation of the following: NERC independent oversight processes and activities, NERC oversight of delegated authority to the Regional Entities, and program development and collaboration with the Regional Entities related to risk-based CMEP and utilization of compliance planning, processes, tools and templates.

The scope of the audit engagement included select areas of the ROP based on risk and significance to CMEP, such as: Risk Assessment/Monitoring/Programs/Tools; Training and Learning Programs and Outreach. In addition, several programmatic plans and reports were reviewed and evaluated which included, but was not limited to ERO Enterprise CMEP Implementation Plan (CMEP IP), annual NERC Oversight Plan, and CMEP Annual Report.

- We noted the following as strengths to support the evolution of risk-based CMEP, adapting to new enterprise processes and technology: Training and learning programs were developed to support the Align implementation and release strategy, which included diverse learning programs and tools: webinars, workshops, training modules, recorded sessions and user guides, and ample training materials posted on nerc.com
- A train-the-trainer program was designed and implemented for Align. NERC and Regional Entities designated subject matter experts as the train-the-trainers, and it was their obligation to provide the subsequent training to internal Regional Entity staff and registered entity staff.
- Numerous program development and collaboration projects and routines were established between NERC and the Regional Entities, which included the formation of task forces and collaboration groups focused on improving program processes and tools

During the course of the audit, we identified thematic opportunities for NERC Compliance and Enforcement to demonstrate and increase the level of oversight across CMEP commensurate with their focus on program development and improvement. For example, we observed strong collaboration with risk assessment processes by partnering with Regional Entities to co-develop CMEP IP and risk elements. However, oversight activities to ensure the effectiveness and inclusion of risk elements by the Regional Entity across the footprint of registered entities was not demonstrated. In addition, the performance of on-going risk assessment activities by Regional Entities during the development of annual audit plans, compliance planning (i.e. IRA, Compliance Oversight Plan development) and compliance monitoring activities was not sufficiently evidenced within the oversight strategy. In respect to Enforcement processes, we observed a focus on compliance and reporting. Overall, CMEP oversight of programmatic reviews and improvements with Regional Entities should be increased.

Extensive collaborative efforts have been demonstrated over the past 24 months to improve risk-based CMEP. Overall, we recommend that NERC CMEP staff establish oversight activities that are demonstrated through monthly, quarterly and annual governance activities, and through existing collaboration groups and routines. Effective oversight and purposeful collaboration will enable consistent assessment and execution of CMEP.

Throughout the audit, NERC Enforcement and Compliance Assurance staff were accommodating and responsive to requests, and the support and professionalism expressed to the audit team contributed to a productive 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), through NERC's oversight, program development, and training and learning programs.

Audit Period and Scope

The period under review was January 1, 2020 through June 30, 2022.

The scope included the following:

- Risk Assessment/Monitoring/Programs/Tools
  - CMEP IP/Risk Elements
  - Inherent Risk Assessments (IRAs)
  - Compliance Oversight Plans (COPs)
  - Annual Audit Planning and Reporting
  - Internal Controls
  - Compliance Investigations
  - Complaints
- Enforcement
  - Analysis, tracking, reporting
  - Dispositions (incl. Dismissals)
  - Penalty program and reviews
  - Self-logging program
  - Sanctions and Remedial Action Directives
  - Hearing and Appeal Procedures
- Training and Learning Programs
  - Delegation
  - Development
  - Delivery/Tracking
- Outreach
  - Strategy/Approach
  - Practice/Implementation Guides
- Technical Feasibility Exceptions (TFEs)
  - Process and Reporting
- Systems, Applications/ITGC

Observation Summary

		Ratings		
Area	**High**	**Medium**	**Low**	**Total**
Risk Assessment/ Monitoring/ Program/Tools	1	3	0	4
Enforcement	0	1	0	1
Training and Learning Programs	0	1	0	1
Outreach	0	0	1	1
TFEs	0	1	0	1
Systems, Applications/ ITGC	0	0	1	1
Total	**1**	**6**	**2**	**9**

High/Medium/Low-Risk Rated Observations

(High, medium, and low risk observations require a management action plan)

Observation	Risk	Rating
Risk management and oversight activities have not been demonstrated, encompassing risk assessment processes, audit planning and execution, through compliance planning and tool utilization	Oversight of CMEP is not effective in ensuring reliability and security due to the limited oversight activities	High
The Complaints process is manual in nature, and revealed discrepancies between the source record, population, and status of Complaints	Complaints may not be identified, assessed and concluded timely in accordance with the ROP, allowing risks, control or compliance issues to adversely impact personnel, operations and potentially the BPS	Medium
Review and evaluation of Annual Audit Plans and execution is not performed	Compliance audit coverage is ineffective to address BPS risks posed by various registered entities having significant impact to the BPS	Medium
Oversight activities related to timely completion of compliance audits and reporting are not consistently performed	Gaps with the execution and completion of compliance audits adversely impact reliability and security Monitoring of the performance and conclusions of compliance audits is ineffective, and delays in sharing results limits learnings with other entities and/or is not in compliance with Appendix 4C, section 4.1.5	Medium
NERC provides limited oversight of the Regional Entities in the administration of the Self-Logging Program	Eligibility, enrollment, and reporting activities within the Self-Logging program is inconsistent, adversely impacting the effectiveness and value of the program	Medium
Formalize Training and Learning Programs and ensure concepts are consistently applied through oversight and collaboration activities	Personnel are not equipped to perform CMEP responsibilities effectively and sustainability relevant to the current environment	Medium
Access to Technical Feasibility Exceptions (TFEs) data and information is not adequately safeguarded	Data and information is inadvertently or intentionally compromised and exploited through procedural and/or access vulnerabilities	Medium
Align issues or potential enhancements are not captured in a way to determine criticality to business process or prioritized to establish level of effort or budget requirements	Issues and delayed enhancements adversely impact CMEP user experience and reduce business process effectiveness	Low
The application and effectiveness of Practice Guides is not evaluated after issuance as part of NERC's oversight activities	CMEP Practice Guides and the intended purpose of each guide are not effective, and lead to inconsistency of use across the ERO Enterprise	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
1	**Risk Assessment, Monitoring, Program, Tools** ROP Section 402; Section 401.6 Risk Elements; CMEP IP ROP Appendix 4C, Section 3.0 NERC Oversight Plan 2021/2022 RDA Section 7 Delegation-Related Activities	**Risk management and oversight activities have not been demonstrated** Oversight activities, for example, in the form of monitoring or inspection, are not performed over Regional Entities to demonstrate review of registered entities by size/risk they pose to the BPS based on registered functions/interconnections/performance considerations, etc. Oversight that demonstrates focus on emerging risks, technical and impact wise to BPS (i.e. supply chain, Distributed Energy Resources, Load….) was not evidenced. Overall, core program elements and tools are developed collaboratively, and independent oversight to assess effectiveness is not evidenced for the following: • CMEP IP/Annual Risk Elements; aggregate view, and not insight across Regional Entities for application and/or inclusion of areas of focus into: ○ Inherent Risk Assessments ○ Compliance Oversight Plans ○ Monitoring activities • Internal controls understanding, identification and assessment by Regional Entities as part of their monitoring activities	NERC Compliance Assurance (NERC CA) will collaborate with Regional Entities, primarily through the Risk Performance Management Group (RPMG), to ensure risk management expectations are established, and NERC CA staff develop oversight engagements with clear objectives around the usage of: • The Annual CMEP IP • Inherent Risk Assessments • Compliance Oversight Plans NERC CA will establish a three year plan to focus these oversight activities. Key outputs: • Clarify Regional Entity expectations • Update NERC CA Oversight Plan MAP Due Date: December 31, 2023	NERC Director of Compliance Assurance and Certification NERC Senior Manager Compliance Assurance	High

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		In accordance with oversight responsibilities, NERC should oversee each Regional Entity that has been delegated authority, to ensure the performance of its obligations under the CMEP. Oversight by NERC shall be accomplished through an annual CMEP review, program audits, and regular evaluations of Regional Entity CMEP performance metrics, risk-based monitoring activities, and performance reports. In addition, NERC has oversight of how Regional Entity specific risk elements related to Reliability Standards are prioritized for registered entity oversight. Effectiveness of CMEP is reduced due to the limited oversight activities in the focus areas noted above. Oversight and training should ensure that risk elements, IRAs/COPs, internal controls, and monitoring activities are enhanced, and performed throughout the year, in addition to annual CMEP Workshops. NERC's oversight should aid in the effectiveness of each of these focus areas and increase the maturity level across Regional Entities.			

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
2	**Risk Assessment, Monitoring, Program, Tools** ROP Appendix 4C Section 4.7.1 Complaint Process; and Section 4.7.2 Anonymous Complaint Notification Procedure	**The Complaints process is manual in nature, and revealed discrepancies between the source record, accuracy of population and status of Complaints** Manual processes over Complaint logging, tracking and resolution creates gaps with NERC oversight of Regional Entity generated complaints and responsibility over anonymous Complaints handling and disposition. Through inquiry with management and inspection of Complaint records, the following was identified: • Two source records were provided for the period under audit (2020 and 2021/2022 Complaint logs) and were not reconciled to reflect overall status and disposition • 2020 Complaint log was retained on a company laptop by an employee who left NERC, and not saved on within the central repository • Two Complaints from 2020 source record do not indicate status or final disposition Effective Complaint processes and handling is a significant enabler to Compliance activities or risk understanding, which is one of the three required components of an ERO compliance	NERC CA will establish a documented process outlining the Complaint tracking process. The process development will include evaluation of technology to automate the tracking, trending, and processing of Complaints, as well as the development of internal controls for ensuring the process performs as expected. MAP Due Date: September 30, 2023	NERC Senior Manager Compliance Assurance NERC Senior Engineer of Reliability Assurance and Certification	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		program. NERC retains the discretion to review any Complaint or to direct a Regional Entity to review a Complaint. The appropriate Compliance Enforcement Authority (i.e. NERC or Regional Entity) is to document the Complaint and the Complaint review, and whether another compliance monitoring or enforcement process is warranted. Complaints may not be identified, assessed and resolved timely in accordance with the ROP, allowing risks, control or compliance issues to adversely impact personnel, operations and potentially the BPS. NERC should evaluate automation capabilities that provide a reliable record or inventory of Complaints, to ensure timely identification, assessment and resolution. In addition, automation may provide capabilities to identify trends or themes that require broader action across the ERO Enterprise that prevent non-compliance or adverse impact to operations.			
3	**Risk Assessment, Monitoring, Program, Tools – Compliance Audit**	**Review and Evaluation of Annual Compliance Audit Plans and Execution is not performed** Through inquiry and observation, IA identified oversight gaps related to compliance audit planning, coverage and execution of	NERC CA will establish a documented process outlining the Regional Entity compliance monitoring schedule tracking process. The process development will include evaluation of	NERC Senior Manager Compliance Assurance CIP Assurance Advisor	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
	Planning and Execution ROP Appendix 4C; Section 4.1 Compliance Audits; Section 4.1.1 Compliance Audit Process; Section 4.1.2 Frequency of Compliance Audits 2021 NERC Oversight Plan	compliance audits performed by the Regional Entities. Examples are as follows: • Identified discrepancy between ERO Compliance Monitoring Schedules and NERC's 3 year validation source record for period under audit; must rely on manual process for completeness and accuracy of source documents • Lack of NERC review of methodology and coverage of compliance audits beyond 3-year audit cycle for BA, RC and TOP functions • Compliance audits were not observed (onsite or offsite) by NERC in 2021 • Two of six audits observed in 2020 did not evidence feedback to the Regional Entities • 2022 audits observed from July, August and September, did not evidence feedback to the Regional Entities to date There is no formal process or reporting application currently used to ensure that the 3-year validation is performed in its entirety and is driven by only one source document completed by the Regional Entities. The 2021 NERC Oversight Plan states that NERC CA staff will continue to observe Regional compliance monitoring engagements in 2021,	technology to automate the tracking of Regional Entity compliance monitoring execution. The automation should consider ROP validations, reporting, and ensuring feedback is shared with Regional Entity staff in a timely manner. This MAP will be informed by the work in the MAP for observation 1 above, particularly as it relates to holistic risk considerations. MAP Due Date: December 31, 2023		

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		and provide feedback at least annually, and in a real time or timely manner depending on issues identified during the engagement. Based on the manual process, errors of omissions may cause non-compliance with 3-year audit cycle requirement. In addition, Compliance audit coverage may not holistically address risks posed by registered entities with functions other than BA, RC, and TOP that significantly impact BPS reliability and security. NERC oversight should include: • Visibility to Regional Entity audit methodology, planning and monitoring that demonstrates holistic, risk-based coverage of all registered entities within the Regional Entity footprint • Observing Critical Infrastructure Protection (CIP) and Operations & Planning (O&P) compliance engagements of Regional Entities annually • Consideration of a reporting application such as SQL instead of manual data entry on spreadsheets • Providing audit feedback to Regional Entities within a reasonable time after each audit engagement observed			

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
4	**Risk Assessment, Monitoring, Program, Tools** ROP Appendix 4C Section 4.1.5 Compliance Audit Reports Regional Entity-led Compliance Audit Report Procedure	**Oversight activities related to timely completion of Regional Entity compliance audits and reporting are not consistently performed (Partial repeat audit issue)** Through inspection of Regional Entity compliance audit reports during the period of our audit, we identified: • 32 audit reports received by the Regional Entities as having no enforcement action, have not been posted as required; the timeframe for posting was approximately 2 years • 61 public audit reports are pending NERC management review prior to public posting • The timeframe from NERC received a nonpublic compliance audit report to when NERC shared the audit report with FERC was approximately 12-24 months While the ROP does not indicate a timeframe for posting audit reports or sharing audit reports with FERC, the timeframes identified are extended and indicate an ad-hoc process. In addition, the extended time frames do not align to NERC's 'Regional Entity-led Compliance Audit Report Procedure' of posting public reports, and sending nonpublic reports to FERC by the end of following quarter of receipt of	NERC CA will update the existing procedure to include additional controls to ensure the process effectiveness. In addition, NERC CA is actively publicly posting the delayed reports and evaluating technology to introduce possible automation for tracking, notifications, and visibility. MAP Due Date: March 31, 2023	NERC Senior Manager Compliance Assurance	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		report. The procedure was developed to address a previous audit observation from the CMEP 2019 audit related to timely receipt, review and sharing/posting of compliance audit reports. Internal processes and procedure are not adhered to, or monitored to ensure effective execution, and delays in sharing results limits learnings with other entities and/or is not in compliance with Appendix 4C, section 4.1.5. Further, the current process of including the topic of compliance audit reports and status on quarterly compliance monitoring calls is not creating transparency and a sense of urgency. NERC should consider: • Establishing a communication routine with each Regional Entity to obtain visibility into the status of compliance audits/reports • Implement a process to ensure internal procedure and protocol is followed • Verify the date the audit report is posted and include on the source document as a means of tracking to meet expectations • Potential updates to Appendix 4C of the ROP to include timelines for posting public audit reports and sending audit reports to FERC for			

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		structure, consistency and awareness to promote transparency and related educational benefits for industry			
5	**Enforcement Self-Logging** ROP, Appendix 4C Section 4.5A; Self-Logging User Guide	**Oversight of applications to and eligibility for Self-Logging program is not performed** Through inquiry of NERC Enforcement personnel, the following oversight activities are not performed related to Self-Logging: • Periodic review of registered entity applications and eligibility activities performed by Regional Entities • Establishing a process to periodically validate the timely submission of self-logs by registered entities to Regional Entity based on approved frequency Note: The Align functionality does not facilitate the identification of required log frequency. Therefore, the majority of Regional Entities receive single submissions real-time vs. batch log. • In addition, there is the capability for registered entities to be partially enrolled in self-logging program, however, the process is manual and not systematically controlled through Align Self-Logging eligibility requirements are established and require a registered entity to demonstrate the ability to identify, assess, and	**Tracking of partial self-logging privileges:** NERC Enforcement has moved its notes regarding partial self-logging privileges for registered entities into Align, specifically to the self-logging entities tracking report. NERC Enforcement is informed of changes to self-logging privileges at monthly calls with Regional Entities and via revocations in settlement agreements or other disposition methods. Implemented as of October 26, 2022 **2023 oversight activity:** NERC Enforcement will conduct a Self-Logging oversight activity in 2023, to among other things, evaluate each Regional Entity's application process, eligibility criteria, review	**Tracking of partial self-logging privileges:** NERC Senior Compliance Enforcement Advisor **2023 oversight activity:** NERC Senior Compliance Enforcement Advisor	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		correct non-compliance during application. Also, approved registered entities are required to submit logs within a stated frequency of three or six months. All non-compliance logged in this manner is presumed to be minimal risk and resolved as a Compliance Exception, provided that the Regional Entity agrees that the noncompliance is a minimal risk and otherwise appropriate for CE treatment. NERC and the Regional Entity discuss self-logged noncompliance that may not be appropriate for CE treatment. Without oversight activities performed, program eligibility requirements and enrollment decisions, and log submissions could be inconsistently applied or determined, creating the perception of unfairness and impact the attractiveness and effectiveness of the program. Also, no monitoring control over timely submission of logs or partial enrollments may allow program requirements to be altered. NERC Enforcement activities related to Self-Logging are more program development and collaborative with Regional Entities. In addition, Align does not provide the capability to identify frequency by registered entity of logs/submissions or those with partial enrollment privileges. Align functionality allows self-logs to be batched or single submitted.	practices to approve enrollment, and timeliness of submissions. MAP Due Date: Commence in Q2 2023 and conclude by December 31, 2023. **Other activity:** NERC Enforcement will work with the ERO Enterprise Enforcement Group to reevaluate the program in light of recent FERC orders. MAP Due Date: Commence in Q2 2023 and conclude by December 31, 2023.		

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		At a minimum, NERC should provide oversight to periodically review Regional Entity eligibility criteria and approval decisions for consistency and fairness.			
6	**Training and Learning Programs** CMEP Annual Report; NERC Oversight Plan; ERO Enterprise Compliance Monitoring Master Training Plan; ROP Section 402.9 NERC Oversight of the Compliance Monitoring and Enforcement Program – Auditor Training	**Formalize Training and Learning Programs and ensure concepts are consistently applied through oversight and collaboration activities** As a result of inquiry with management, and inspection of training and learning program documentation, we observed the following: • A need to validate that concepts are applied from training and learning programs focused on areas such as risk elements, risk factors, risk categories, and the development/completion/ understanding of IRA/COPs and Internal Controls • CMEP department staff training and learning programs for new hires are not formalized to include documentation to support tracking by employee • A NERC CA CIP staff observed an audit for a registered entity during the audit period, without completion of the required auditor training; and took approximately 5 months from hire date to complete the courses	NERC Enforcement will formalize its onboarding training, including tracking completion by new hires. MAP Due Date: June 30, 2023 NERC CA will formalize an onboarding checklist, including implementing controls to ensure completion of required training prior to performing oversight responsibilities. In addition to the onboarding checklist, NERC CA will develop a periodic training evaluation process. This will ensure NERC CA staff periodically receive the necessary training to effectively perform BPS reliability and security oversight.	**NERC Enforcement Response:** NERC Manager, Compliance Analysis, Reporting, and Tracking NERC Senior Counsel **NERC CA Response:** NERC Senior Manager Compliance Assurance	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
	RDA Section 7(e) Training and Education; 8 (b) Oversight of Performance of Delegated Functions and Related Activities ROP Section 900 Training and Education	NERC CMEP staff is to provide training to ERO Enterprise staff through workshops, instructor-led training events, and eLearning opportunities. These opportunities focus on identifying gaps in staff knowledge and capabilities related to the risk-based CMEP. Training and educational opportunities concerning Reliability Standards, compliance monitoring and enforcement processes, and other supporting reliability functional areas are provided to other NERC staff, Regional Entity staff, and industry participants at various events through the year. The ERO Enterprise Compliance Monitoring Master Training Plan states that the Foundations of Auditing (FOA) course is required for ERO Enterprise audit team members or observers before attending an audit as a team member or observer. NERC stated they have a checklist for staff that includes the required auditor training but training was not monitored. Without training and learning program documentation, personnel may not receive the guidance to perform their CMEP responsibilities effectively. NERC should develop a training and learning program strategy to assist in prioritizing and	MAP Due Date: September 30, 2023		

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		addressing more comprehensive needs based on oversight activities. NERC CA should monitor staff training to ensure completion of required training. In addition, NERC CMEP should develop a formal training program for new CMEP hires to deliver the required training including verification of completion.			
7	**Technical Feasibility Exceptions (TFEs)** ROP, Appendix 4D, Section 13.1 Annual Report to FERC and Other Applicable Governmental Authorities	**Access to Technical Feasibility Exceptions (TFEs) data and information is not adequately safeguarded** Through inquiry with management and observation of the TFE process, we identified the following data and information control weaknesses: Access to TFE data in Align extends to users that do not have a business purpose for review or reporting responsibilities • Approximately 40 NERC staff have access to Align TFE data. Five Standards personnel do not have a business need for this access. Data is exported from Align to develop a log of TFEs required to create and submit an annual TFE report to FERC • NERC staff exports the TFE data to desktop and prepares the report for	NERC CA will formalize the process, to include controls to ensure data confidentiality. NERC CA staff is working with IT to better understand the access controls and permissions in Align. NERC staff will work with NERC IT on appropriate access provisioning and rights that are based on business function and purpose. MAP Due Date: June 30, 2023	Lonnie Ratliff, Director of Compliance Assurance and Certification Davis Jelusich, CIP Compliance Advisor	Medium

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		posting to a secure NERC central repository Per the ROP, Appendix 4D, Section 13.1, NERC is required to submit an Annual Report to FERC that provides analysis regarding the use of TFEs and the impact on the reliability of the Bulk Electric System. Access to data and processing should be established based on role provisioning and business purpose. In addition, desktop files and backups should be properly purged based on procedure and systematic or monitoring controls. Improper user access provisioning may allow TFE data and information to be compromised. Further, downloading data to a laptop reduces visibility to and security of the data, increasing vulnerability of an inadvertent or intentional data breach. NERC should review role provisioning to confirm access is granted based on business purpose, and remove access as appropriate for users without a business purpose. In addition, NERC should develop a procedure to ensure consistency and monitoring over processes to remove files from desktop, hard drive and/or a secure NERC central repository upon creation and submission of the annual report to FERC. The central repository for TFE data should			

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		remain within Align and be restricted to those with a business purpose.			
8	**Systems, Applications/ IT General Controls (ITGCs)** **GTAG1:** Information Technology Controls apply to all systems, components, processes, and data for a given organization or IT environment. ITGCs ensure the proper development and implementation of applications, as well as the integrity of programs,	**Align issues or potential enhancements are not prioritized and communicated based on criticality to business process and users** Through inquiry with NERC management, internal management routines are in place to record potential issues and enhancements from Align implementation releases of functionality. However, through observation and inspection, the following was identified: • Approximately 700 Align enhancements are recorded on a Prioritization Critical List source document; 10% (70) of which are considered critical issues • Two quarterly Align User Group (AUG) sessions were conducted in 14 months as awareness to the broader stakeholder group • Awareness and communication of Release 2 and Release 3 as Pilot Programs was limited As releases are implemented, a process to capture feedback and/or gauge effectiveness of the user community should be implemented within a reasonable frequency. Existing governance or communication routines should be leveraged to ensure system and user	NERC is preparing for the transition to the governance model and proactively determining the correct communication paths, including moving the Align webpage to the CMEP section of the NERC website and having CMEP staff ensure communications are timely and accurate. MAP Due Date: June 30, 2023	NERC Senior Compliance Enforcement Advisor NERC Compliance Assurance Engineer	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
	data files, and computer operations. Align User Group Charter	functionality, and process and control issues are addressed. NERC has focused on timeliness of Align releases, and logging issues and enhancements for future action once all releases are implemented. Further, technical issues are addressed separately by helpdesk tickets and not included on the backlog list. Last, Align User Group routines have not been formally conducted due to the continuation of Steering Committee routines beyond Q2 2022. Upon transition to the Align/SEL governance model, the Align Product Management Team should review the enhancements and issues log with input and prioritization considered from the Operations Leadership Team (OLT) in support of criticality to business processes and business users that impact effectiveness of the program. In addition, NERC CMEP should re-evaluate the frequency of management routines and establish communication protocols to ensure participation within the AUG represents feedback from the Align user community related to system and process issues.			

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
9	**Outreach** NERC Oversight Plan	**The application and effectiveness of Practice Guides is not evaluated after issuance as part of NERC's oversight activities** NERC has established a monitoring/ validation mechanism with the Regional Entities to ensure the objectives of practice guides are understood and learnings are consistently applied, and not in conflict with compliance auditing procedures. However, the mechanism is not utilized. NERC provided examples from 2020 oversight templates used for audit observations of registered entities that included to 'make a determination of ERO Enterprise compliance monitoring approaches and/or CMEP Practice Guides,' however, responses within the template for individual registered entities, and feedback surveys provided from 2020 did not include specifics related to Practice Guides. Limited compliance audits were observed by NERC during 2020 – 2022, therefore, real-time oversight of the application and understanding of Practice Guides did not occur to the degree necessary across the ERO Enterprise. In addition, other collaboration routines with Regional Entities did not demonstrate a focus on, or requests for feedback related to the	NERC CA has established consistency issue reporting tools in place. The ERO Enterprise Program Alignment Process is outlined on the NERC website and is intended to provide industry the opportunity to report perceived inconsistencies in the approach, method, or practices employed by ERO Enterprise CMEP staff. NERC CA will provide additional awareness of the Program Alignment Process. MAP Due Date: March 31, 2023	NERC Senior Manager, Compliance Assurance NERC Senior Compliance Assurance Advisor	Low

Observation #	Location/ Control/ROP Reference	Observation	Management Action Plan (MAP) and Due Date	Responsible Person(s)	Impact
		application and effectiveness of the Practice Guides. Without a reliable mechanism to periodically evaluate/monitor the CMEP Practice Guides, the intended purpose of each guide may not be effective and lead to inconsistency of use across the ERO Enterprise. NERC should provide training and establish a communication protocol for each practice guide released, and expand oversight beyond observed audits. Oversight should consist of establishing processes or periodic routines, including communication protocols, to evaluate consistent application, relevance and overall effectiveness.			

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.