

RELIABILITY & SECURITY

Oversight Monthly Update

Formerly the Compliance Open Webinar

January 19, 2023





Reliability & Security Oversight Monthly Update

January 19, 2023

Mailee Cook
Training and Outreach
Specialist

Save the Date

- March 7–8, 2023: Board of Directors and Associated Meetings
- March 21, 2023: Virtual Reliability & Security Workshop

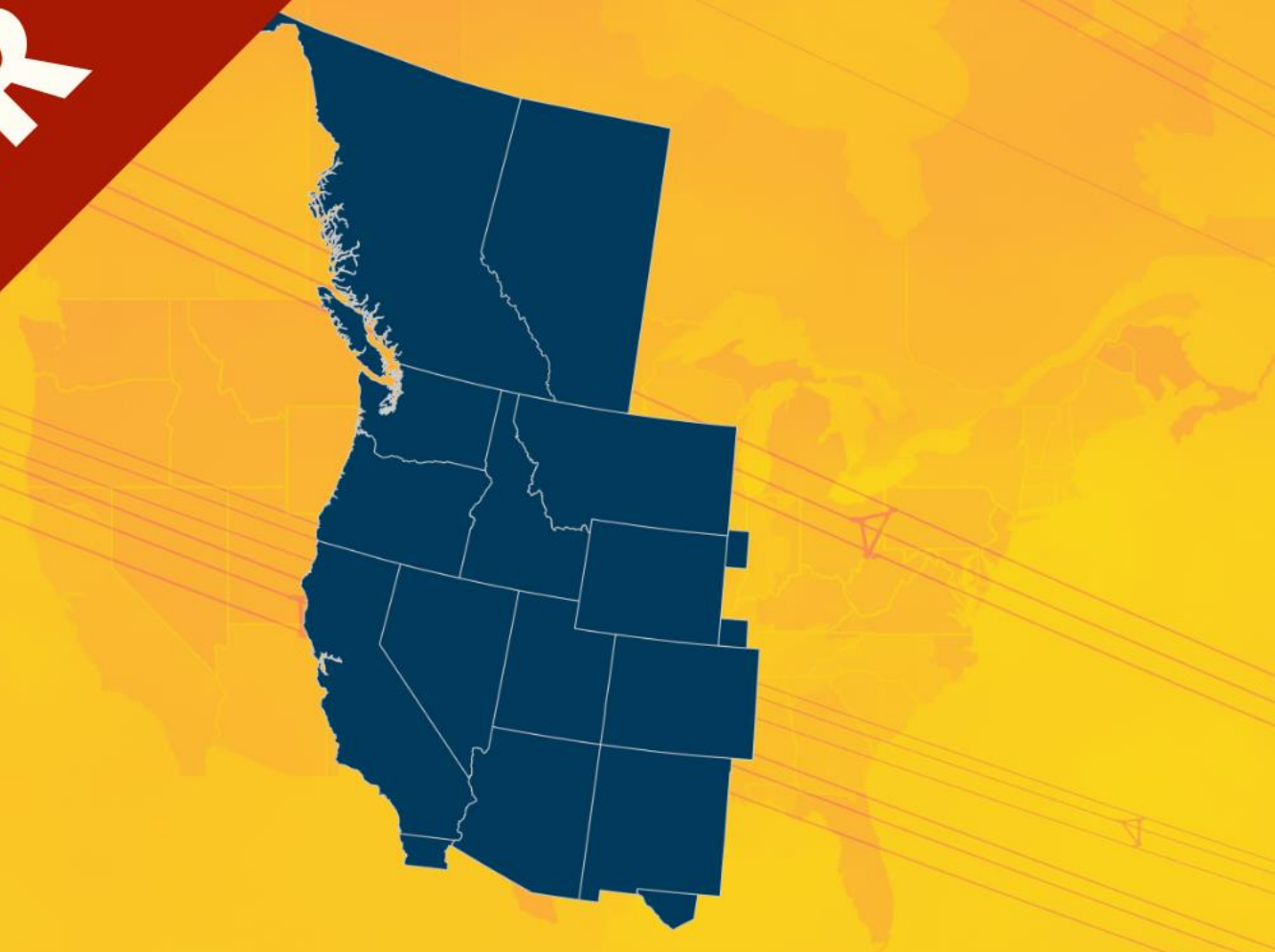




RESOURCE ADEQUACY

DISCUSSION SERIES

WEBINAR



WESTERN ASSESSMENT

of Resource Adequacy





Grid *FUNDAMENTALS*

February 21–22, 2023



Oversight Quarterly Trends Report

- Provides insights into oversight trends in the Western Interconnection.
- The first [report](#) is live on wecc.org.



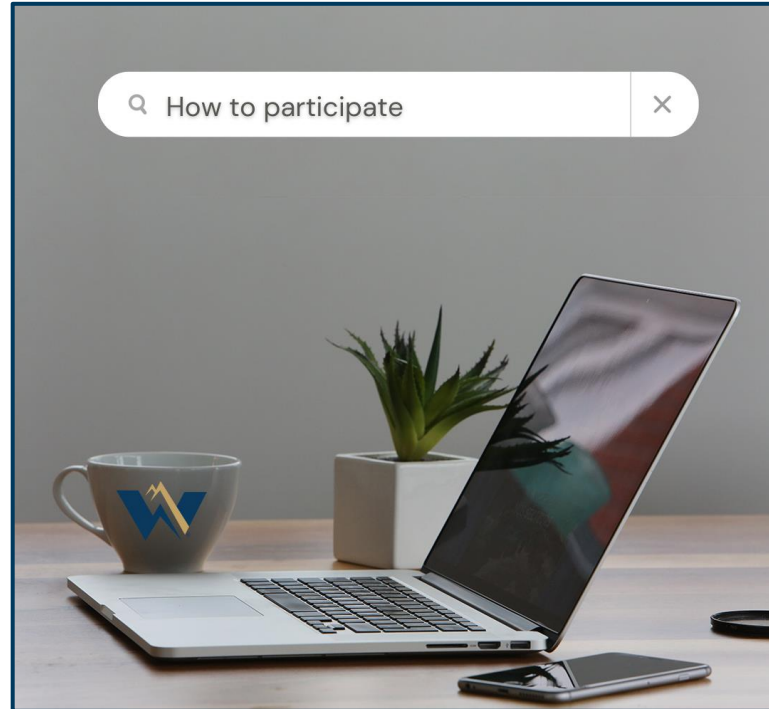
Antitrust Policy

- All WECC meetings are conducted in accordance with the WECC Antitrust Policy and the NERC Antitrust Compliance Guidelines
- All participants must comply with the policy and guidelines
- This meeting is public—confidential or proprietary information should not be discussed in open session

Antitrust Policy

- This webinar is being recorded and will be posted publicly
- By participating, you give your consent for your name, voice, image, and likeness to be included in that recording
- WECC strives to ensure the information presented today is accurate and reflects the views of WECC
- However, all interpretations and positions are subject to change
- If you have any questions, please contact WECC's legal counsel

Participating



Send questions via chat to WECC Meetings
Use the “raise hand” feature

Agenda

- **Noncompliance Mitigation**
 - **Michael Dalebout, Manager of Enforcement Operations**



Noncompliance Mitigation

January 2023

Michael Dalebout
Manager of Enforcement
Operations

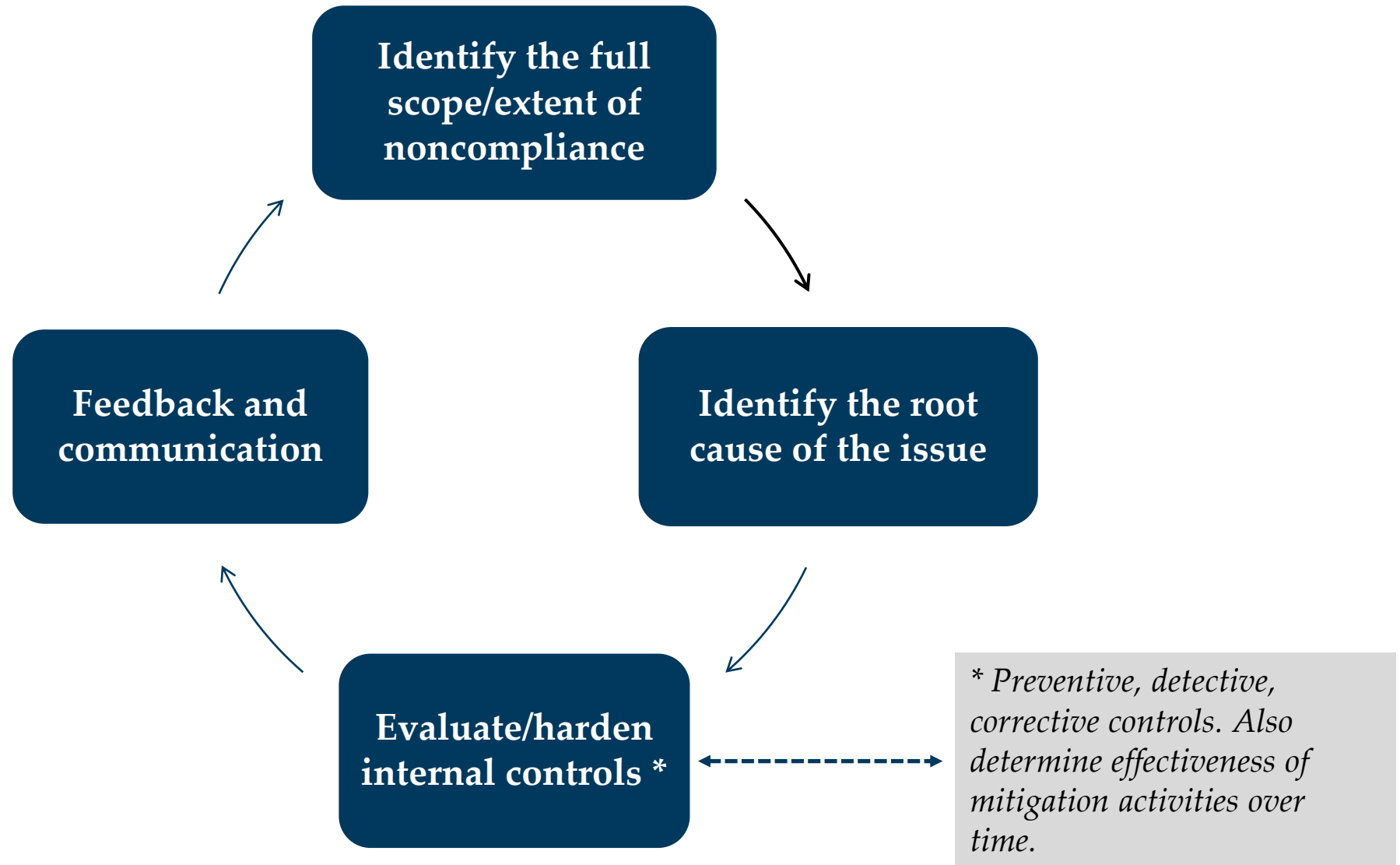
Noncompliance Mitigation

- Mitigation Defined
- Cycle of Mitigation
- Mitigating Activities (MA) and Mitigation Plans (MP)
- WECC Processing Goals
- Training Opportunities & Resources
- Questions

Mitigation

Mitigation describes the corrective actions taken to address noncompliance, preventive actions to avoid recurrence, and internal controls to reduce future risk.

Cycle of Mitigation



Mitigation Plan vs. Mitigating Activities



Mitigation Plan vs. Mitigating Activities

Key Differences



Mitigation Plan vs. Mitigating Activities

Requirement	Mitigation Plan	Mitigating Activity
Actions & Tasks	Formal action plan with documented milestones	List of tasks the entity expects to complete by a set date
Milestones	Needs milestones for future activities that are no more than three months apart. CEA has the authority to check in and request updates on each milestone	No milestones required, but entities should ideally complete tasks within 12 months. The CEA may inquire periodically about the progress
Expected Completion	Needs an expected completion date—cannot be before the last milestone date	Needs an expected completion date and a justification for the time needed to complete the activities
Duration	Formal action plan with documented milestones	List of tasks the entity expects to complete by a set date

Mitigation Plan vs. Mitigating Activities

Requirement	Mitigation Plan	Mitigating Activity
Documentation	Formal process that is bound by the CMEP requirements for timely submittals, review, and acceptance. Also submitted to FERC as a stand-alone document	Informal process where the tasks to be completed are typically included in the disposition document. Review and approval is performed as part of the disposition of the noncompliance. No separate submittal to FERC outside of the final disposition
Completion	Certification of completion and evidence supporting completion of mitigation by the registered entity is required. The CEA may then choose how to verify depending on the risk and disposition and will issue a formal verification of completion document	No formal certification of completion required from the registered entity, but it would still need to notify the CEA of the actual completion date and provide evidence of completion as instructed by its CEA. The CEA may choose to verify, but verification is not required

Mitigation Plan vs. Mitigating Activities

Requirement	Mitigation Plan	Mitigating Activity
Controls	Entities required to implement preventive, detective, and corrective controls with the primary intent to detect the noncompliance in advance and to prevent it or reduce the likelihood of recurrence	Entities encouraged to review and report on the preventive, detective, and corrective controls associated with the noncompliance
Disposition Track	Typically used for moderate or serious risk violations that CEAs process as Spreadsheet NOPs or Full NOPs	Typically used for minimal and some moderate risk issues that are processed as Compliance Exceptions or FFTs. Nevertheless, a CEA may permit robust and well-described mitigating activities for all risk levels— including noncompliance posing a serious or substantial risk to the reliability and security of the BPS

Mitigation Submittal Requirements



Mitigation Key Differences

Contents	Mitigation Plan	Mitigating Activity
Extent of condition and description of the noncompliance	Required to be included in the Mitigation Plan—even if included in other documents	Not separately required if included in the Self-Report document
Cause of the noncompliance	Required to be included in the Mitigation Plan—even if included in other documents	Not separately required if included in the Self-Report document
Corrective actions	Required to be included in the Mitigation Plan—even if included in other documents	Required
Detective, Preventive, & Corrective Actions	Required to be included in the Mitigation Plan—even if included in other documents	Required

Mitigation Key Differences

Contents	Mitigation Plan	Mitigating Activity
Milestones*	Required (if mitigation extends more than three months into the future)	Required
Proposed Completion Date	Required	Required
Interim Risk Reduction	Required to be included in the Mitigation Plan—even if included in other documents	Not separately required if included in the Self-Report document
Prevention of Future Risk to Reliability	Required to be included in the Mitigation Plan—even if included in other documents	Not separately required if included in the Self-Report document

** Milestones should include corrective and remediating actions or controls with the primary intent to remediate the noncompliance and restore compliance with the Reliability Standard(s) as quickly as possible; as well as preventive and detective actions or controls to detect the noncompliance and prevent it or reduce the likelihood of recurrence.*

CE Mitigation Policy Clarifications

Remediation Evidence

Entities are not required to submit evidence of remediation for Compliance Exceptions.

CE Mitigation Plans

Mitigation must be complete or completed within 12 months for Compliance Exceptions.

CE Mitigation Evidence

Minimal risk PNCs processed as Compliance Exceptions do not need evidence of Remediation and Mitigation verified unless requested.

WECC Processing Goals

Metric	Goal
% inventory with unknown remediation status	20%
% mitigation approved within 180 days of intake	80%

Training Opportunities & Resources



Align Training on Demand



<https://training.nerc.net/>


Registered Entity User Guide

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Registered Entity Self-Report and Mitigation Plan User Guide

January 04, 2021

RELIABILITY | ACCOUNTABILITY



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

Appendix B: Self-Report Checklist

The intent of this checklist is to provide a quick outline of the topics discussed in *Chapter 1: Description of the Noncompliance*. Entities in the Self-Logging Program can also use the following checklist.

- Does the Self-Report describe the discovery of the noncompliance?
 - How was the noncompliance discovered and when did the noncompliance occur?
 - Was it discovered by an internal employee or a third party?
 - Was it discovered through self-evaluation, internal review or investigation, or the internal compliance program?
 - Was it discovered through detective controls? If so, explain how the detective control led to the discovery of the noncompliance, provide an explanation of the detective control's adequacy, and discuss if it needs improvement to detect similar issues earlier.
 - Was it discovered in preparation for, or during, a Compliance Monitoring engagement (i.e., Audit, Spot-Check, Self-Certification, etc.)?
 - Was it discovered during the implementation of mitigating activities for an open enforcement action?
 - Was it revealed through an event or other operational occurrence?
 - What date did the entity discover the noncompliance?
 - What period elapsed between identifying and reporting the noncompliance to the CEA? If there is a gap exceeding three months between identifying the noncompliance and reporting the noncompliance to the CEA, is there an explanation?
 - Has the same or similar noncompliance been previously reported or reported to other CEAs?
- Does the Self-Report describe the noncompliance?
 - Is the noncompliance adequately described by tying the description to the Reliability Standard/Requirement?
 - Does the description include how the noncompliance occurred? What happened (how were the Standard and Requirement violated), why it happened (cause), where it happened (type of Facility, location of Facility, etc.), and how it happened (facts and circumstances surrounding the noncompliance)?
 - Has an extent of condition review been performed, and if so, what other processes, procedures, controls, assets, facilities, or personnel were impacted or could be impacted by the noncompliance?
- Does the Self-Report describe the cause of the noncompliance?
 - Has the cause been completely identified?
 - What was the sequence of events that led to the issue?
 - Why did the issue develop as it did?
 - Is the sequence of events logical? Does it represent an accurate picture of what happened?
 - Is this issue just a symptom of a potentially larger problem?
 - With respect to the cause of the noncompliance, were there extenuating circumstances?
 - What type of preventive or detective controls were in place at the time of the noncompliance, if any?
 - If there were controls in place, explain how the controls were or were not effective.
 - Is there a corrective control that would mitigate the noncompliance? If so, what?
- Does the Self-Report include duration information?
 - What date did the noncompliance begin? What date did the noncompliance end? Include an explanation for those dates, if known.
- Does the Self-Report address the risk associated with the noncompliance?

NERC | Registered Entity Self-Report and Mitigation User Guide | January 2021

40

Appendix C: Mitigation Checklist

Checklist

A quick outline of the topics discussed in *Chapter 3: Mitigation of the Noncompliance* and *Chapter 4: Mitigation of the Noncompliance in Align*. The registered entity should identify which is applicable and where the information will appear in the Self-Report.

- act
- Mitigation Plan, is a Registered Entity Contact specified?
- If the noncompliance being mitigated.
- ely described by tying the description to the Reliability Standard?
- ow the noncompliance occurred?
- discovered? Did the registered entity discover the noncompliance using
- in changed from what was originally reported (e.g., additional
- und to be in scope)? Did the registered entity consider all procedures,
- hel that were directly impacted or could be impacted by the
- pliance.
- y identified?
- ting causes?
- discovered by the registered entity, did the entity review its detective
- hing needs to be improved or implemented?
- ewed its own compliance history to see if a same or similar issue has
- nd prevention of recurrence actions.
- ements in scope?
- ise of the noncompliance?
- been addressed?
- solve the noncompliance and reasonably prevent recurrence been
- actions completed prior to submission of the plan been included?
- where appropriate?
- ded, do the milestones have sufficient detail?
- rivals reasonable?
- rivals no longer than three months apart?
- to provide proof of completion for all actions taken.
- te.
- ed prior to the proposed plan completion date?
- ated with the reliability of the BPS while the mitigation is being
- terim steps to address this risk?

- Describe the prevention of future risk to the reliability and security of the BPS.

NERC | Registered Entity Self-Report and Mitigation User Guide | January 2021

42



Align Self-Report and Mitigation Guide
WECC Enforcement and Mitigation
May 2021

Use this guide when entering a potential noncompliance (PNC) in Align. For more information on submitting Self-Reports and Mitigation, please see the [NERC Registered Entity Self-Report and Mitigation Plan User Guide](#).¹

Fields on Finding Form in Align

The Finding form in Align is where a registered entity can Self-Report or Self-Log a PNC. An asterisk at the end of the field name indicates a required field.

General Information

Field Name	Description
Registration	Populates with NERC Compliance Registry (NCR) information for the selected registered entity.
Applicable Requirement	Populates with the selected Standard and Requirement; select the applicable current effective Standard and Requirement, even if the PNC began under an earlier version.
Applicable Part(s)	Prepopulates with all parts; remove any that do not apply to the PNC.
Applicable Reliability Function	Prepopulates with NCR's registered functions; remove any that do not apply to the PNC.
Region – Jurisdiction in which the Potential Noncompliance occurred	Prepopulates with Compliance Enforcement Authority (CEA) associated with the NCR (i.e., WECC).
Other Region – Jurisdiction(s) where you are reporting this Potential Noncompliance	[Dropdown Field] Select all other applicable regions.

¹ <https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Registered%20Entity%20Self-Report%20and%20Mitigation%20Plan.pdf>

155 North 400 West | Suite 200 | Salt Lake City, Utah 84103
www.wecc.org

Appendix B: Self-Report Checklist

Appendix B: Self-Report Checklist

The intent of this checklist is to provide a quick outline of the topics discussed in *Chapter 1: Description of the Noncompliance*. Entities in the Self-Logging Program can also use the following checklist.

- Does the Self-Report describe the discovery of the noncompliance?
 - ✓ How was the noncompliance discovered and when did the noncompliance occur?
 - Was it discovered by an internal employee or a third party?
 - Was it discovered through self-evaluation, internal review or investigation, or the internal compliance program?
 - Was it discovered through detective controls? If so, explain how the detective control led to the discovery of the noncompliance, provide an explanation of the detective control's adequacy, and discuss if it needs improvement to detect similar issues earlier.
 - Was it discovered in preparation for, or during, a Compliance Monitoring engagement (i.e., Audit, Spot-Check, Self-Certification, etc.)?
 - Was it discovered during the implementation of mitigating activities for an open enforcement action?
 - Was it revealed through an event or other operational occurrence?
 - ✓ What date did the entity discover the noncompliance?
 - ✓ What period elapsed between identifying and reporting the noncompliance to the CEA? If there is a gap exceeding three months between identifying the noncompliance and reporting the noncompliance to the CEA, is there an explanation?
 - ✓ Has the same or similar noncompliance been previously reported or reported to other CEAs?
- Does the Self-Report describe the noncompliance?
 - ✓ Is the noncompliance adequately described by tying the description to the Reliability Standard/Requirement?
 - ✓ Does the description include how the noncompliance occurred? What happened (how were the Standard and Requirement violated), why it happened (cause), where it happened (type of Facility, location of Facility, etc.), and how it happened (facts and circumstances surrounding the noncompliance)?
 - ✓ Has an extent of condition review been performed, and if so, what other processes, procedures, controls, assets, facilities, or personnel were impacted or could be impacted by the noncompliance?
- Does the Self-Report describe the cause of the noncompliance?
 - ✓ Has the cause been completely identified?
 - ✓ What was the sequence of events that led to the issue?
 - ✓ Why did the issue develop as it did?
 - ✓ Is the sequence of events logical? Does it represent an accurate picture of what happened?
 - ✓ Is this issue just a symptom of a potentially larger problem?
 - ✓ With respect to the cause of the noncompliance, were there extenuating circumstances?
 - ✓ What type of preventive or detective controls were in place at the time of the noncompliance, if any?
 - If there were controls in place, explain how the controls were or were not effective.
 - Is there a corrective control that would mitigate the noncompliance? If so, what?
- Does the Self-Report include duration information?
 - ✓ What date did the noncompliance begin? What date did the noncompliance end? Include an explanation for those dates, if known.
- Does the Self-Report address the risk associated with the noncompliance?

NERC | Registered Entity Self-Report and Mitigation User Guide | January 2021

Appendix C: Mitigation Checklist

Checklist

quick outline of the topics discussed in *Chapter 3: Mitigation of the Chapter 4: Mitigation of the Noncompliance in Align*. The registered identify which is applicable and where the information will appear in

act
litigation Plan, is a Registered Entity Contact specified?
f the noncompliance being mitigated.
ely described by tying the description to the Reliability Standard?
ow the noncompliance occurred?
discovered? Did the registered entity discover the noncompliance using

in changed from what was originally reported (e.g., additional
und to be in scope)? Did the registered entity consider all procedures,
hel that were directly impacted or could be impacted by the

pliance.
y identified?
iting causes?
discovered by the registered entity, did the entity review its detective
thing needs to be improved or implemented?
ewed its own compliance history to see if a same or similar issue has

nd prevention of recurrence actions.
 ements in scope?
 use of the noncompliance?

actions completed prior to submission of the plan been included?

where appropriate?
 ded, do the milestones have sufficient detail?
 rivals reasonable?
 rivals no longer than three months apart?
 to provide proof of completion for all actions taken
 te.
 te prior to the proposed plan completion date?
 ated with the reliability of the BPS while the n
 terim steps to address this risk?

- Describe the prevention of future risk to the reliability and security of the BPS

NERC | Registered Entity Self-Report and Mitigation User Guide | January 2021
42

Appendix 4C to the Rules of Procedure

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	
Compliance Monitoring and Enforcement Program	
Appendix 4C to the Rules of Procedure	
Effective: May 19, 2022	
Table of Contents	
1.0	INTRODUCTION4
2.0	COMMUNICATION WITH ORGANIZATIONS RESPONSIBLE FOR COMPLYING WITH RELIABILITY STANDARDS.....4
3.0	ANNUAL IMPLEMENTATION PLAN4
4.0	COMPLIANCE MONITORING PROCESSES.....4
4.1	Compliance Audits.....5
4.2	Self-Certifications10
4.3	Spot Checks.....10
4.4	Compliance Investigations11
4.5	Self-Reports.....14
4.5A	Self-Logging.....14
4.6	Periodic Data Submittals14
4.7	Complaints15
4.8	Preliminary Screen16
4A.0	ENFORCEMENT DISCRETION17
4A.1	Compliance Exception Process17
4A.2	FFT Process17
5.0	ENFORCEMENT ACTIONS.....18
5.1	Assessment of Potential Noncompliance19
5.2	Notice of Preliminary Screen19
5.3	Notification to Registered Entity of Alleged Violation19
5.4	Registered Entity Response.....20
5.5	Hearing Process for Compliance Hearings21
5.6	Settlement Process.....21

RELIABILITY | RESILIENCE | SECURITY

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	
1.0 INTRODUCTION	
This Compliance Monitoring and Enforcement Program ("CMEP") is the program to be used by the North American Electric Reliability Corporation ("NERC") and the Regional Entities to monitor, assess, and enforce compliance with Reliability Standards within the United States. The CMEP will also be implemented in Canada and Mexico consistent with laws and agreements in effect with Applicable Governmental Authorities.	
Capitalized terms used in this appendix shall have the meanings set forth in Appendix 2 of the NERC Rules of Procedure.	
2.0 COMMUNICATION WITH ORGANIZATIONS RESPONSIBLE FOR COMPLYING WITH RELIABILITY STANDARDS	
The Compliance Enforcement Authority ("CEA") shall require each Registered Entity to designate a contact person(s) responsible for sending and receiving all necessary information and communications concerning CMEP matters. The CEA will designate where Registered Entities are to send CMEP-related correspondence.	
3.0 ANNUAL IMPLEMENTATION PLAN	
NERC and the Regional Entities will maintain and update an ERO CMEP Implementation Plan, which reflects ERO and Regional Entity-specific risk elements related to the Reliability Standards that CEAs should prioritize for oversight of Registered Entities.	
NERC posts the ERO CMEP Implementation Plan on the NERC website on or about November 1 of the calendar year preceding implementation. NERC and the Regional Entities may update and revise the ERO CMEP Implementation Plan during the course of the calendar year of implementation, as necessary, to reflect changing risk elements and prioritization of oversight activities.	
NERC, with input from the Regional Entities, stakeholders, and regulators, shall identify risk elements and related NERC Reliability Standards and Requirements to be considered in the annual ERO CMEP Implementation Plan for oversight of Registered Entities. In order to identify risk elements, NERC will consider data including, but not limited to: emerging risks; compliance findings; event analysis experience; data analysis; and the expert judgment of NERC and Regional Entity staff, committees, and subcommittees. NERC uses these risk elements to identify and prioritize continent-wide risks to the reliability of the Bulk Power System.	
4.0 COMPLIANCE MONITORING PROCESSES	
The CEA will monitor Registered Entities' compliance with Reliability Standards using the compliance monitoring processes described herein. A CEA will determine the type and frequency of compliance monitoring process to apply based on the Registered Entity's specific risks to the reliability of the Bulk Power System.	
If a compliance monitoring process reveals a potential noncompliance with a Reliability Standard, the CEA will conduct a Preliminary Screen of the potential noncompliance in accordance with Section 4.8. If the	
Appendix 4C to the NERC Rules of Procedure	4

decision will not be held in abeyance and will be considered as repeat

Rejection of Proposed Mitigation Plans

If the CEA, it will complete its review of the Mitigation Plan, and will reject the Mitigation Plan, within sixty (60) days of receipt; deemed accepted. In order to extend the initial or an extended period CEA shall, within the initial or extended review period, notify the CEA (if not the CEA) that the review period is being extended and identify its review of the Mitigation Plan. The CEA's extension notice shall be a notice by the end of the extended review period either stating that the Mitigation Plan or further extending the CEA's period for review of the Mitigation Plan will be deemed accepted.

If the CEA will provide the Registered Entity with a written statement and will require the Registered Entity to submit a revised Mitigation Plan will notify the Registered Entity within thirty (30) days after receipt of the CEA will accept or reject the revised Mitigation Plan and provide a written statement for rejection and the Required Date for the second revised Mitigation Plan of extension of the review period. If the CEA does not accept the Mitigation Plan within 30 days after receipt of a revised Mitigation Plan, the CEA will accept the Mitigation Plan. If the second review results in rejection of the Mitigation Plan, the CEA will issue a written statement accepting a Mitigation Plan.

If the Regional Entity accepts a Mitigation Plan, the Regional Entity (i) will provide the Mitigation Plan and (ii) will provide the accepted Mitigation Plan to the CEA for review. The CEA will review the accepted Mitigation Plan and, within sixty (60) days of receipt of the Mitigation Plan from the Regional Entity, will notify the Regional Entity and the CEA, as to whether the Mitigation Plan is approved or disapproved. If the Mitigation Plan is disapproved, the CEA will reject the Mitigation Plan that was accepted by the Regional Entity. NERC shall may state the changes to the Mitigation Plan that would result in the Mitigation Plan shall not be subject to findings of violations of the specific Reliability Standards that are the subject of the Mitigation Plan or to imposition of Penalties. The CEA will reject the Mitigation Plan if the Mitigation Plan was under consideration following NERC's disapproval of the Mitigation Plan, so long as the modified Mitigation Plan that addresses the concerns identified by

Mitigation Plans

rejected in accordance with its terms. At the CEA's discretion, the CEA may reject a Mitigation Plan for good cause including, but not limited to: (i) operational issues

Future Enforcement Training

Training Topic	Date
Extent of Condition Training	February 9, 2023 2:00–3:00 p.m. MTN
Root Cause Training	March 2, 2023 2:00–3:00 p.m. MTN
Mitigation through Internal Controls	April 6, 2023 2:00–3:00 p.m. MTN

Contact:

Michael Dalebout

Manager of Enforcement Operations

mdalebout@wecc.org

RELIABILITY & SECURITY

Oversight Monthly Update

Formerly the Compliance Open Webinar

February 16, 2023 2:00 pm MT





Follow and engage!
@weccreliability