NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Registered Entity Self-Report and Mitigation Plan User Guide

October 15, 2024

RELIABILITY | ACCOUNTABILITY




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

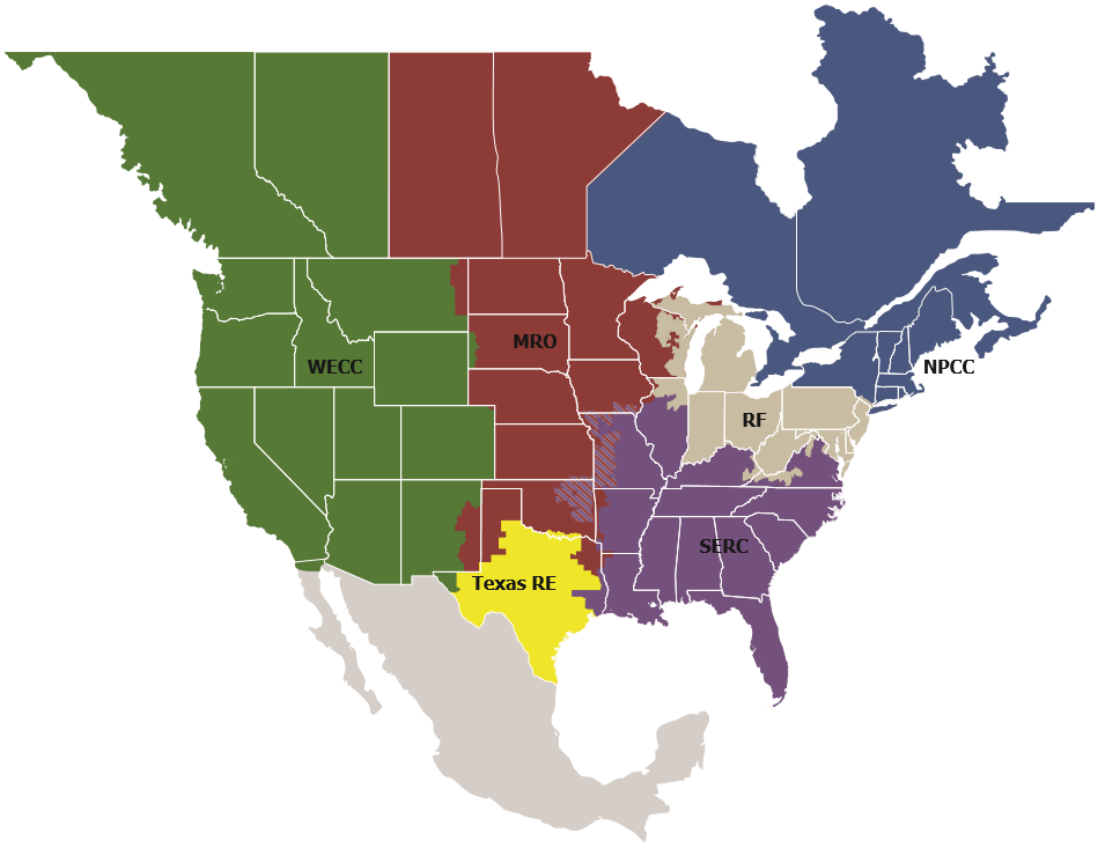
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Disclaimer

The guidance contained in this document represents suggestions on particular topics that Registered Entities should apply according to the individual facts and circumstances surrounding specific instances of noncompliance. This guidance does not create binding norms, establish mandatory Reliability Standards, or create parameters to monitor or enforce compliance with Reliability Standards. This guidance provides information and advice for Registered Entities to use when reporting instances of noncompliance[1] to their Compliance Enforcement Authority (CEA).[2]

[1] As used in this document, noncompliance could mean potential noncompliance or confirmed noncompliance.

[2] As there are updates to the Align system, the changes will not be automatically reflected in this User Guide until the next revision. The release notes are posted on the NERC Align webpage for users' awareness.

Document Revisions

Date	Version Number	Document Changes
January 17, 2014	1.0	
April 17, 2014	2.0	Multiple revisions based on comments received during public comment period, January 22, 2014, through February 21, 2014.
June 12, 2018	3.0	This document is a consolidation of the 2014 Mitigation Plan User Guide, the 2014 Self-Report User Guide, and the 2012 Self-Report Guidance document. Multiple revisions based on comments received from a joint NERC, Regional Entities, and industry taskforce, as well as NERC and Regional Entities working groups.
January 4, 2021	4.0	Updated with additional guidance as it applies to the Align and Secure Evidence Locker environment implementation. Multiple revisions based on comments received from NERC, Regional Entities working groups, and Compliance and Certification Committee (CCC).
October 15, 2024	5.0	Periodic review to reflect latest processes, including updates to Finding, Risk and Mitigation sections. Multiple revisions based on comments received from NERC, Regional Entity working group, and CCC.

Introduction

The ERO Enterprise developed this User Guide for Registered Entities' use in reporting and mitigating noncompliance. The purpose of this document is to describe the type and quality of information that the Registered Entity must submit to allow for an effective evaluation by the CEA[3] regarding the circumstances and risk of a noncompliance and the activities a Registered Entity takes to address them. The ability of the CEA to arrive at a final disposition determination in an efficient and effective manner depends on the quality of the information it has about the facts of the noncompliance, risk, cause, and related mitigation. Accordingly, this User Guide provides guidance to assist Registered Entities with the submission of Self-Reports/Self-Logs and mitigating activities. The content in this guide is applicable to both Self-Reports and Self-Logs.[4] For additional guidance on the Self-Logging program, the Registered Entity should review the Self-Logging Program User Guide.[5]

In Align,[6] the Registered Entity will submit the Self-Report and may submit mitigation activities at the same time via the mitigation milestones form. If the Registered Entity does not submit mitigation activities with the Self-Report in Align, the Registered Entity is able to submit mitigation later.

This guide supplements information provided in the NERC Compliance Monitoring and Enforcement Program (CMEP), Rules of Procedure (ROP), Appendix 4C.[7,]

This User Guide is organized as follows:

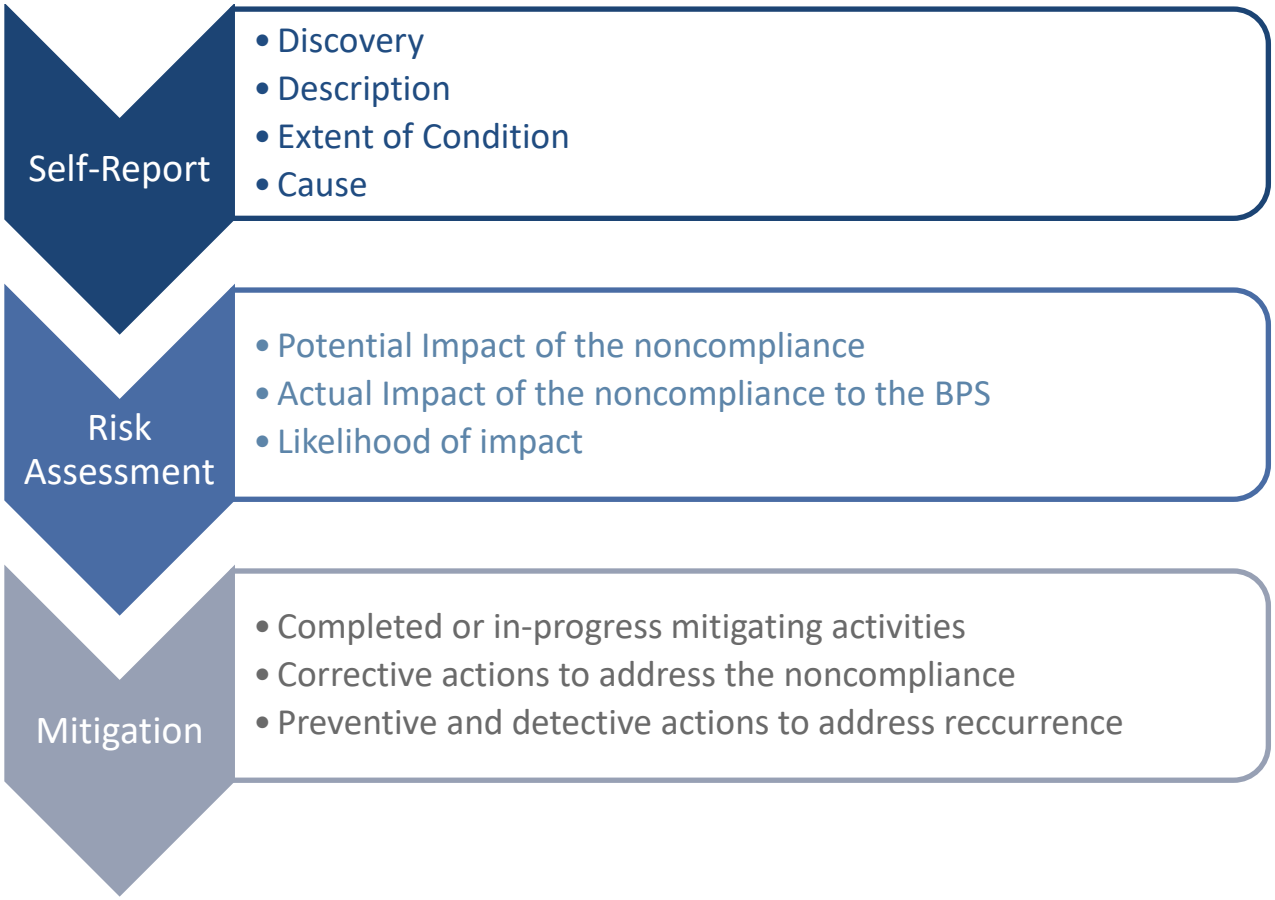
[3] "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

[4] As used in this document, references to Self-Report could also be applicable to Self-Log.

[5] The Self-Logging Program User Guide.

[6] Align is a tool that has positioned the core CMEP business processes of NERC and the Regional Entities on a single, secure platform that includes functionality related to Enforcement and Mitigation, Periodic Data Submittals, Technical Feasibility Exceptions, Self-Certifications, Audits, Spot Checks, Inherent Risk Assessment, and Compliance Oversight Plans.

[7] The NERC Rules of Procedure.


Self-Report
• Discovery
• Description
• Extent of Condition
• Cause
Risk Assessment
• Potential Impact of the noncompliance
• Actual Impact of the noncompliance to the BPS
• Likelihood of impact
Mitigation
• Completed or in-progress mitigating activities
• Corrective actions to address the noncompliance
• Preventive and detective actions to address reccurrence

Chapter 1: Description of the Noncompliance

Prompt and accurate self-reporting is integral to identifying, mitigating, and preventing repeat noncompliance. In evaluating Self-Reports and mitigating activities, CEAs consider the individual facts and circumstances surrounding each instance of noncompliance. This User Guide discusses some of the key points the CEA considers when reviewing the reported noncompliance and mitigating activities.

Providing adequate, accurate, and relevant information in a Self-Report enables efficient and timely resolution of instances of noncompliance. Registered Entities should submit Self-Reports based on preliminary information in a timely manner, as soon as practical but typically within three months of discovery,[8] and provide more comprehensive information to the CEA as it becomes known. Further, if the Registered Entity is unsure whether it is noncompliant with a Reliability Standard, it is best practice to contact the CEA for a preliminary discussion. The NERC Sanction Guidelines direct CEAs to consider whether the Registered Entity submitted a Self-Report and whether the Registered Entity voluntarily undertook corrective action.

Although this chapter discusses the relevant information that the Registered Entity should include in a Self-Report, the Registered Entity should consider this guidance whenever it submits any noncompliance-related information to the CEA.

Important Details for Noncompliance

Including sufficient information in Self-Reports is essential for the CEA to evaluate the issue, determine if a noncompliance exists, and assess the risk it poses to the reliability and security of the BPS. Detailed information within the Self-Report may also result in an earlier decision about disposition.[9] The CEA may consider how long it took the Registered Entity to discover after the issue occurred and how long it took the Registered Entity to submit the Self-Report after discovery. If the Registered Entity is in the process of identifying all relevant information and the process may take more than three months to complete, the Registered Entity should inform its CEA of the noncompliance and ask for guidance on the timing for the Self-Report submittal. The Registered Entity should retain all records that could potentially be associated with the noncompliance until it receives notice from the CEA.

In Align, the Registered Entity should submit mitigating activities either (1) as part of the Self-Report at the time of submittal of the Self-Report to the CEA or (2) as a separate submission through the Mitigation Management module at a later date. The Registered Entity can submit the mitigating activities with the Self-Report if all milestones are identified at that time, otherwise the Registered Entity should wait until it has identified all the milestones to submit the mitigating activities.

Description of the Discovery of the Noncompliance

In its Self-Report, the Registered Entity should describe how and when it discovered the noncompliance. The Registered Entity should also note if the noncompliance relates to a previous Self-Report, is a result of an internal review preparation following a Compliance Monitoring notification, and if it was reported to other CEAs. If the Registered Entity has sensitive information, it should upload that information into the ERO Secure Evidence Locker (ERO SEL) instead of including it in the Self-Report form in Align.[10] Sensitive information may include: IP addresses,

[8] As discussed below, undue delay in self-reporting may affect how the CEA determines disposition and penalty.

[9] The Registered Entity can view the steps to create and submit a Self-Report by reviewing the Align Enforcement and Mitigation User Guide located on the NERC Training site.

[10] ERO SEL or SEL refers to the secure evidence locker, which provides enhanced security in evidence collection via a NERC on-premises environment. The use of the SEL is only for activities associated with the content in Align.

Vulnerability Assessments, lists of high impact Bulk Electric System (BES) Cyber Systems (BCSs), lists of medium impact BCS, list of Electronic Security Perimeters (ESPs), *etc.*[11]

The CEA will review the facts that pertain to a Registered Entity's discovery of noncompliance. An adequate Self-Report should answer the following questions:

1. How and when did the Registered Entity discover the noncompliance?
    a. Was it discovered by an internal employee or a third party?
    b. Was it discovered through self-evaluation, internal review or investigation, or an internal compliance program (*e.g.*, internal controls)?
        i. If discovered through detective controls, explain how the detective control led to the discovery of the noncompliance. In addition, the Registered Entity should provide an explanation of the detective control's function and adequacy, and whether it needs improvement to detect similar issues earlier.
    c. Was it discovered in preparation for, or during, a Compliance Monitoring engagement (*i.e.*, Audit, Spot Check, Self-Certification)?[12]
    d. Was it discovered during the implementation of mitigating activities for an open enforcement action? The Registered Entity could discuss with the CEA if it should submit a Finding Update to the open enforcement action or if it should submit a new Self-Report.
    e. Was it revealed through an event or other operational occurrence?
        i. If discovered due to an event, provide the date of that event and, if applicable, the category of the event.[13]
    f. What date did the Registered Entity discover the noncompliance? If there is a gap exceeding three months between identifying the noncompliance and reporting the noncompliance to the CEA, explain.
2. Has the Registered Entity or affiliates previously reported a same or similar noncompliance to the same or other CEA(s)?
    a. If so, include the date submitted, NCR of the submitting Registered Entity, Align Unique ID for that finding, and recipient CEA(s).

Description of the Noncompliance

In its Self-Report, the Registered Entity should include all relevant details surrounding the noncompliance and should provide the necessary details to explain how the Registered Entity violated the Standard and Requirement. If the Registered Entity has sensitive information, it should upload that information into the ERO SEL instead of including it in the Self-Report form in Align.[14]

For the CEA to evaluate a reported noncompliance, a Registered Entity should include at least the following information in its Self-Report:

[11] *See* "Data Handling in Align and the SEL" reference document for additional guidance on the types of information that might need to be submitted in the SEL instead of Align.

[12] The Registered Entity should submit a Self-Report at any time, but if it is in preparation for a Compliance Monitoring engagement, the Registered Entity should indicate that in the discovery details. When assessing a penalty, the CEA will determine if the Registered Entity should receive "credit" for submitting the Self-Report. *See also, North American Electric Reliability Corporation*, 134 FERC ¶ 61,209 (2011) (Turlock Order).

[13] *See* Event Analysis Program document.

[14] *See* n.8.

1. The Reliability Standard and Requirement, as well as all sub-Requirement(s) at issue, and the registered functions at issue. A separate Self-Report should be created for each Requirement with the noncompliance information relevant only to that Requirement.
2. If the noncompliance started under a previous version of the Reliability Standard and Requirement, the Registered Entity can provide that information in the detailed description. In Align, Registered Entities should submit noncompliance under the current effective Standard. For example, if a noncompliance regarding access management has a start date of October 1, 2015, and was reported in March 2024, the Registered Entity would report the noncompliance occurred under CIP-004-,6 as that is the version of the Reliability Standard that was in effect at the time of submitting the noncompliance to the CEA.[15]
3. 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)?
    a. This should include identification of the nature and extent of condition (EOC) of the noncompliance, including, but not limited to: the number of total affected employees, the type of affected systems (*e.g.*, relays, current transformers (CTs)/potential transformers (PTs), batteries.), and the number of Cyber Assets and descriptions, intervals, and other relevant portions. As a guide for what type of information would be beneficial in describing the noncompliance, the Registered Entity can review the Reliability Standard/Requirement, the measures in the Standard, the Reliability Standard Audit Worksheet, the Violation Severity Level, and the Implementation Plan.
    b. The size, nature, criticality, and location of the facility or assets where the noncompliance occurred.
    c. The number of assets that were at issue, the nature and function of the asset(s), and the total population of assets. For CIP-specific noncompliance, include the location of affected Cyber Assets (*e.g.*, within an ESP or Physical Security Perimeter (PSP), Control Center),type of Cyber Asset (*e.g.*, BES Cyber Asset, Protected Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System), and the impact level (*e.g.*, High Impact, Medium Impact). If the Registered Entity has sensitive information, it should upload that information into the ERO SEL instead of including it in the Self-Report form in Align. Information in Align should be sufficient for processing of compliance and enforcement records.
    d. The Registered Entity should assess its compliance history with this Standard and Requirement and explain whether this noncompliance is a repeat issue. If it is a repeat issue, explain why the issue occurred after the prior Mitigation.
4. Identify if any processes, procedures, controls, *etc.* did not operate as intended resulting in the noncompliance.
5. Identify the duration of the noncompliance, including start and end dates, and an explanation for those dates, if known. The start date is the earliest known occurrence of the noncompliance, the enforceable date of the Standard, registration date, or the prior mitigation completion date for the same Standard and Requirement. The end date is when the Registered Entity corrected the noncompliance (*i.e.,* remediated), which is not necessarily the mitigation completion date.

[15] In the noncompliance submittal, the Registered Entity would include the correct start date even if that date is tied to a prior version of the Standard.

Extent of Condition of the Noncompliance, if known

Establishing the EOC is integral to developing successful mitigating activities. The extent of the review may differ based on the facts of the noncompliance. If the Registered Entity does not identify the full EOC of the noncompliance, the likelihood for repeat occurrences increases. The purpose of performing an EOC analysis is to provide reasonable assurance that the Registered Entity has identified all effects from the underlying noncompliance so that its remediation efforts are comprehensive, therefore, lessening the risk of potential harm to the BPS. The Registered Entity may discuss the level of EOC review that is appropriate with the CEA.

If a Registered Entity determines that performing the EOC review would hinder notification to the CEA of the noncompliance in a timely manner, then this step can be included within the mitigating activities after the EOC review is completed. In the Self-Report, the Registered Entity may indicate that the EOC review has been completed, in progress, or not completed.

In all cases, no matter if a Registered Entity performs the EOC review at the time of discovery or through the mitigation of the noncompliance, the CEA expects a Registered Entity to identify the EOC of the noncompliance and communicate this to the CEA in a timely manner.

The CEA and NERC should be able to understand how the Registered Entity determined that the level of EOC review was appropriate. The Registered Entity should include how the EOC was performed (*e.g.,* automated tools, manual reviews, sampling) and what evidence the Registered Entity reviewed. For example, if the Registered Entity can show noncompliance occurred with a brand of relay only used in one substation, there may be no need to consider all other facilities.

Therefore, the Registered Entity needs to provide the details of the EOC review and an explanation as to how the Registered Entity determined the correct EOC. If there are any concerns about whether the EOC review is thorough enough, the Registered Entity should contact the CEA to discuss the risk and reasonableness of the review. If the CEA and Registered Entity determine that an EOC review is not required or that a more limited review should be performed based on its preliminary assessment of the compliance, the Registered Entity should provide the reason(s) for not performing one. This is particularly true for a noncompliance that, based on information provided to the CEA early in the enforcement process, is isolated and minimal risk.

Depending on the nature of the noncompliance, the Registered Entity could consider the following as part of determining the EOC of the noncompliance:

1. Other affiliate companies or facilities across its corporate structure, including those registered in other Regions.
2. Procedures, assets, facilities, or personnel that are directly affected or could be affected as part of the noncompliance.
3. Other Reliability Standards, to determine if additional ones were also violated based on the facts of the reported noncompliance.
4. Prior compliance history involving similar conduct or similar gap in internal controls, if known; and
5. Whether the EOC changed from what was originally reported (*e.g.*, additional devices/facilities/personnel found to be affected).

If the Registered Entity identifies additional instances of noncompliance related to the same Reliability Standard and Requirement, the Registered Entity should contact the CEA to determine if it should submit a Finding Update to the original Self-Report or submit a new Self-Report.

A Registered Entity should also review the facts and circumstances of the noncompliance to see if any other Reliability Standards could also pertain, which would expand the scope of noncompliance. If the Registered Entity

identifies an additional noncompliance related to other Reliability Standards, the Registered Entity should submit a Self-Report for that instance.

Causes of the Noncompliance

All noncompliance must have the cause(s) identified prior to final disposition. The listed cause(s) of noncompliance should be consistent between the facts of the noncompliance, the risk(s) it posed, and the actions taken to mitigate and reasonably prevent recurrence.

A Registered Entity should identify and include in its Self-Report all cause(s), including the root cause and any contributing causes, of a noncompliance in order to effectively correct the instant issue and reasonably prevent recurrence. The root cause is the most basic reason(s) for a condition or problem which, if eliminated or corrected, would have prevented it from existing or occurring. The contributing cause is the cause that contributed to an event but, by itself, would not have caused the event. In absence of a formal root cause analysis, the entity should use its best judgement to identify the cause(s) that would prevent recurrence of the issue. If identifying the cause(s) would prevent the Registered Entity from notifying the CEA of the noncompliance in a timely manner, then the Registered Entity should include its best estimation of the cause, and the cause analysis[16] process can be part of mitigation. The Registered Entity should identify all contributing causes in order to effectively correct the noncompliance and prevent recurrence. In Align, the Registered Entity is able to select from a list of Enforcement Cause Codes.[17] NERC has created a Cause Coding User Guide to help the Registered Entity in determining the appropriate Enforcement-specific cause code that corresponds to the identified root cause of the noncompliance. Enforcement Cause Codes can be used to help the Registered Entity group similar causes for analysis to determine: whether the issue is a common problem, the frequency of the problem occurring, whether the issue is wide-spread, and whether prior mitigation solutions have been or are being effective.

Thorough causal analysis helps solve issues by attempting to identify the cause(s) of events (*e.g.*, weak key controls for contractors) so that Registered Entities can mitigate those causes, as opposed to simply addressing the symptoms of an issue (*e.g.*, taking away a contractor's key). By focusing correction on causes, the Registered Entity can reduce the likelihood of recurrence. The Registered Entity should perform a causal analysis for all noncompliance, regardless of the discovery method (*i.e.*, Self-Report, Audit, Spot Check, Self-Certification). If the noncompliance is discovered through a Compliance Monitoring activity, then the CEA may identify what it believes to be the root cause of the noncompliance, but the Registered Entity should still conduct its own analysis. This analysis should tie directly to the mitigation activities. In the example of weak key controls, the Registered Entity should consider asking additional "why" questions to determine the underlying cause. **Why did the weak key control exist?** *Because the site in question used an antiquated system different from other sites*. **Why was the system different?** *Because the site was acquired in a merger.* **Why did the old system remain in place?**

Many methods can be used to determine the cause(s) of noncompliance. The guidance[18], "Cause Analysis Methods for NERC, Regional Entities, and Registered Entities," as well as several other references noted in ***Appendix F: Reference Documents,*** provide references to methods and tools routinely used in the investigation, analysis, and determination of causal and contributing causes that drive noncompliance. Regardless of the methods and tools used, Registered Entities should establish a repeatable cause analysis process that they apply consistently when analyzing noncompliance.

[16] "Cause analysis" is a collective term that describes a wide range of approaches, tools, and techniques used to uncover the contributing causes of noncompliance.

[17] The Root Cause Code is a single select field which can be selected by clicking on the search button using the magnifying glass icon and then selecting the radio button for the appropriate cause code. The Contributing Cause Code(s) is a multi-select field and can be selected by clicking on the search button using the magnifying glass icon and then selecting the check boxes for the appropriate cause codes.

[18] Cause Analysis Methods for NERC, Regional Entities, and registered Entities (September 2011).

While there is often overlap between different causes and other areas requiring additional internal controls, and each needs to be explained, the mitigating activities should address the cause(s). Sometimes a "cause and effect" chain (*e.g.*, A caused B, then B caused C, and then C caused the noncompliance) can explain the cause. The Registered Entity should use caution when using a cause-and-effect chain since it can be very narrowly focused. A broader view of the issues can often result in Registered Entity mitigation efforts that more thoroughly address multiple underlying causes.

Human error and lack of training are rarely the appropriate causes of noncompliance. Registered Entities should be able to attribute the cause to something such as insufficient or ineffective internal controls, procedural deficiencies, deficient contractor oversight, or a lack of communication from management, *etc.* Individuals make mistakes, but behavior is typically influenced by organizational processes and values. The majority of training or human error-caused noncompliance can be traced to either failures in management or failures in programs and procedures. The limitations of human performance are well known, so processes and internal controls should be designed accordingly.

Undocumented knowledge, processes, or procedures (*i.e.*, something an employee knows and performs on a regular basis but is not documented) that were not followed because the knowledgeable person was not present can sometimes cause noncompliance. In this case, a Registered Entity should ensure that it documents the processes or procedures and provides training on updated and newly documented procedures to relevant personnel.

When determining causes, it is best to begin by clearly stating what happened, when it happened, and why it happened. Then examine the facts and circumstances for indications as to how the issue developed. To determine the cause of the noncompliance, Registered Entities should consider, at a minimum, the following:

1. What was the sequence of events and/or causes that led to the issue?
2. Why did the issue develop as it did?
3. Is the sequence of events logical? Does it represent an accurate picture of what happened?
4. Is this issue a symptom of a potentially larger problem?
5. With respect to the cause of the noncompliance, were there extenuating circumstances?
6. What type of preventive or detective controls were in place at the time of the noncompliance, if any?
    a. If there were controls in place, explain how the controls were or were not effective.
    b. Is there a corrective control that would mitigate the noncompliance? If so, what?

Coordinated Oversight

Registered Entities in the Coordinated Oversight Program should follow the requirements of the program to identify which CEA should receive the Self-Report and mitigating activities.[19] Nevertheless, the guidance contained in this user document would still apply for these Registered Entities regardless of the CEA receiving the submittal. For Registered Entities, a reporting entity should ensure all fact, risks, and mitigation descriptions refer to the facilities or assets affected by the reported noncompliance with the requirement, even if it pertains to a different registration than that assigned to the reporting entity.

If a Registered Entity is part of the Coordinated Oversight Program, it should report any noncompliance to the Lead Regional Entity (LRE). In Align, the Registered Entity will have the ability to submit a Self-Report and select any additional Coordinated Oversight registrations that are impacted, as well as indicate in which Region the noncompliance occurred. The LRE will coordinate with the Affected Regional Entity (ARE) so there is no need for

[19] Information on the Coordinated Oversight Program for MRREs is available at this location.

duplicate reporting.[20] For Self-Reports related to system-wide operations, system-wide programs, or specific facilities located within the LRE footprint, the LRE will notify the ARE of the self-reported noncompliance, as appropriate and determine the required next steps. For Self-Reports related to specific facilities within the ARE footprint, the LRE will notify the ARE and determine the next steps required. When conducting the EOC review, the Registered Entity should discuss with the LRE how to organize the results of the EOC review. The Registered Entity should look at all of the Registered Entities and facilities that are part of the Coordinated Oversight group.

For Registered Entities that are registered in multiple Regions but not in the Coordinated Oversight Program, the Registered Entity should submit the Self-Report to all CEAs where the noncompliance occurred for each Registered Entity that had the noncompliance.

[20] If the MRRE has any concerns about unnecessary duplication of effort on any future self-reported noncompliance, the MRRE should contact the LRE's staff. The LRE's staff will coordinate with the applicable ARE's staff.

Chapter 2: Risk Assessment

This section describes how Registered Entities may assess the risk to the reliability and security of the BPS posed by noncompliance with a Reliability Standard. The purpose is not to establish a rigid set of criteria, but rather to define certain principles that are useful when assessing risk. Depending on a Registered Entity's size and organizational structure, the nature and complexity of the risk due to similar instances of noncompliance can vary. These guidelines will assist Registered Entities in assessing their own risk in a thorough and consistent manner.

How to Assess Risk

Noncompliance may pose a wide spectrum of risks. The ERO Enterprise refers to risk posed to the reliability or security of the BPS as either **minimal, moderate, or serious**.[21]

Risk is the potential impact to reliability or security multiplied by the likelihood of that impact occurring. Risk assessment involves reviewing the negative consequence or the potential impact of the event and the likelihood that the event will occur, based on the internal controls in place at the time the noncompliance occurred, as well as the inherent risk of the Registered Entity.

The assessment of risk to the reliability and security of the BPS considers a variety of inputs, including the Registered Entity's specific systems, devices, activities, and footprint. The risk also considers any compensating or mitigating factors, as well as internal controls that existed during the period of noncompliance, in addition to any impacts caused by the noncompliance. When a Registered Entity assesses the risk to the reliability and security of the BPS, the Registered Entity should include details that explain the risk posed to the BPS. If the risk is moderate, the Registered Entity should include information to explain why the risk was not serious. If the risk is serious, the Registered Entity should include information to explain why the risk was not lower.

Entities should base risk assessments on facts existing at the time of the noncompliance, and not on assumptions, or facts that develop later. Nevertheless, if a Registered Entity identifies relevant information during its EOC review or mitigation, it should include that information in its risk assessment. A good risk assessment is composed of three steps (1) risk evaluation, (2) factors reducing the risk, and (3) risk of possible recurrence. These steps are detailed below.

Risk Evaluation

The first step in risk assessment is evaluating the potential impact or harm that could have occurred to the facilities, assets, or BPS because of the noncompliance, as well as the likelihood of occurrence. When the Registered Entity evaluates potential impact to the BPS, it should, at a minimum, consider the following factors:

1. What were the system conditions during the event? For example, did the noncompliance take place while the system was stressed, *i.e.*, during an Energy Emergency or when other emergency or special operating procedures were in effect?
    a. The system conditions at the time of the issue, *i.e.,* N-1, Misoperations, extreme weather, and any extenuating circumstances.

[21] Minimal: Nothing serious could have occurred and there were complete or significant protections in place to reduce the risk; alternatively, the impact was insignificant, minor, or limited.
Moderate: Something serious could have occurred and there were only some protections in place to reduce the risk; alternatively, the impact was conspicuous, evident, or noticeable.
Serious: The most serious risk issues are: (i) those involving or resulting in (a) extended outages, (b) loss of load, (c) cascading blackouts, (d) vegetation contacts, (e) systemic or significant performance failures; and (ii) those involving (a) intentional or willful acts or omissions, (b) gross negligence and (c) other misconduct, alternatively, the impact was significant, substantial, or extreme. *See also, North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) at P49.

2. Was there any potential for loss of a Protection System device, degradation or loss of a BES element, loss of a BCS or information, or providing unauthorized access to BCSs?
3. What are the size, nature, criticality, and location of the facilities at issue?
4. What actual impact occurred, what potential impact could have occurred, and what was the likelihood of the potential impact occurring?
5. How many assets were at issue and what was the nature and function of the asset(s) (*e.g.*, the affected assets were a High Impact BCA and a Medium Impact PACS)? Does the affected asset(s) perform a reliability task?
6. What other systems, facilities, or staff are exposed to the same possible failure modes?
7. Were there any Misoperations or exceedances of system operating limits or interconnection reliability operating limits (IROL) during the course of the noncompliance?
8. Was there potential to affect any CIP technical controls that may have impacted BCSs?
9. The time horizon of the noncompliance, *i.e.*, did the noncompliance impair or threaten real-time operations or day-ahead operations planning?[22]
10. Whether the noncompliance was isolated or a systemic/general control failure potentially impacting multiple processes/systems.

Risk assessments should be specific to the Registered Entity, the BPS, and the Registered Entity's existing controls which may mitigate the risk. The Registered Entity should provide details about what risks were associated with the noncompliance at the time it took place. The Registered Entity should not include any assumptions and should not solely rely on a variation of the Reliability Standard's purpose statement to explain the risk. The risk that matters is related to the specific Registered Entity in the specific circumstance, not the risk of the Requirement in general. For example, if the noncompliance was a failure to test a relay within the prescribed maintenance and testing period, the risk should account for what could have happened on the Registered Entity's system if that relay failed during the noncompliance period.

The risk should address whether the noncompliance took place during a time of elevated risk (*i.e.*, an event on the system) and the risk should indicate whether the noncompliance contributed to the event or if it occurred because of the event. The risk should also consider the size and location of the facilities where the noncompliance took place. For instance, if the issue only affected a single generator in a Registered Entity's corporate structure, that should be included to evaluate the full risk of the noncompliance.

The Registered Entity should address how the noncompliance affected the system overall and whether there was any impact to the BPS. To the Registered Entity's knowledge, this would address any negative impact to the facilities, assets, resources, equipment, Cyber Systems, the BPS, *etc.* The Registered Entity needs to provide any relevant information (such as EOC evaluation) to the CEA so it can complete the risk assessment evaluation. If the Registered Entity has sensitive information, the Registered Entity should upload that information into the ERO SEL instead of including it in the Self-Report form in Align.

Factors Reducing the Risk

The second step in risk assessment is to determine the likelihood that the above-identified impact would occur. This likelihood is influenced by factors (*e.g.*, internal controls, size of facilities, early detection, remote electronic access) in place at the time of the noncompliance. The analysis generally involves identifying the duration or EOC of the issue in conjunction with internal controls (*i.e.*, preventive, detective, and corrective controls), or redundancies (*i.e.,* backups or other Registered Entities performing the same function)[23] in place at the time of noncompliance. When the Registered Entity evaluates the likelihood of the impact occurring, it should also

[22] Registered Entities can find information on specific FERC-approved time horizons within the text of each Reliability Standard. Additionally, there is a general definition document on what a time horizon is for a Reliability Standard.

[23] For example, a failure to perform CT maintenance on redundant CTs when the main CTs were tested and maintained in a timely manner.

consider mitigating factors that would have reduced the potential impact of the noncompliance. Among other things, these may include alarms, monitoring activities, back-up or redundant facilities, or other activities. The Registered Entity should include details about any internal controls that were in place that expedited the discovery of the noncompliance, shortened the duration of the noncompliance, or reduced the severity of the impact of the noncompliance. When evaluating risk, the Registered Entities should provide factors that increase as well as decrease the likelihood of actual impact.

If there were internal controls in place, the Registered Entity should describe how effective the Registered Entity's policies, procedures, *etc.* were at preventing, detecting, and correcting the noncompliance prior to the manifestation of harm.

A control could be a process, procedure, system, or a tool and implemented in an automatic or manual manner. Controls will vary from Registered Entity to Registered Entity because no two Registered Entities are alike in system design, configuration, program, business plans, and functions performed. Some examples of controls are:

1. A peer review process;
2. An automatic notification;
3. Frequency and voltage alerts;
4. A generation startup checklist; and
5. Internal audit programs.

The Registered Entity must also include steps that will reduce or eliminate risk to the BPS while it implements mitigation. In determining interim actions and activities, Registered Entities should identify and address any risks to the BPS that may exist while mitigation is in progress. It should also include steps that it has already taken, or which are in place to reduce or eliminate risk to the BPS.

Risk of Possible Recurrence

The third step in the risk assessment is to determine the likelihood of a same or similar noncompliance occurring again. The Registered Entity should take the results of the cause determination into consideration when determining the likelihood of recurrence. As part of mitigation of the current noncompliance, the Registered Entity's EOC review should identify how widespread the issue could have been so that the Registered Entity can discuss the risk posed by recurrence and add controls to reasonably prevent recurrence. For example, if the Registered Entity had a vegetation contact or encroachment due to program deficiencies, the Registered Entity would want to provide the risk posed to other lines using that same program and assess when it last checked those lines to see if there could be possible encroachments. Additionally, evaluation of prior compliance history will provide the Registered Entity with an understanding of whether its mitigating activities were deficient due to a misidentified cause, or another reason, which also might increase or decrease the risk of recurrence. When the Registered Entity evaluates the mitigating factors for the noncompliance, it should consider the following at a minimum:

1. Is the cause of the noncompliance the same as or similar to prior instances of noncompliance?
2. Are the circumstances surrounding the noncompliance rare or common?
3. What remediation steps are already in place to address the issue?
4. What controls will the Registered Entity put into place to reasonably prevent recurrence?
    a. Are the controls implemented Registered Entity-wide?
    b. Are the controls business-function or process driven? Each business function may have different controls in place that may help detect or prevent issues.

For more information of what needs to be included in the mitigation activities to address risk and recurrence, please see ***Interim Risk Reduction*** in Chapter 3.

Chapter 3: Mitigation

In Align, all mitigation starts as mitigating activities. The Registered Entity can create the mitigation milestones on the Self-Report form and submit the milestones at the same time the Registered Entity submits the Self-Report to the CEA. The Registered Entity should only submit the mitigation record if it is ready for the CEA to review. The Registered Entity also has the option to submit mitigation to the CEA under the Mitigation Management module. The Registered Entity should not submit partial mitigation to the CEA as it is not possible to update the milestone description or add new milestones unless the CEA rejects the mitigation record. If the Registered Entity needs to update the mitigation after submission, the Registered Entity should contact the CEA so the mitigation record can be rejected and then updated by the Registered Entity. If, based on review of the Self-Report and mitigating activities, the CEA determines a Mitigation Plan might be necessary, the CEA can request that the Registered Entity resubmit the mitigation as a Mitigation Plan. The biggest difference is that the Mitigation Plan is a documented plan that has specific review timelines and is submitted to FERC after NERC approval per Section 6.0 of Appendix 4C of the NERC ROP.[24] If the Registered Entity has sensitive information, the Registered Entity should upload that information into the ERO SEL instead of including it in the Self-Report form in Align.

If the Registered Entity identifies additional details that are relevant for the noncompliance after it has submitted the Self-Report, the Registered Entity should contact the CEA to determine if it should submit Finding Updates in Align or request the mitigation record be sent back to the Registered Entity for revision, so that the CEA has the most up to date information during its review. While the benefits of Registered Entities submitting more thorough and timely mitigation to CEAs include faster determination of how the CEA should process an issue of noncompliance and faster processing times, it is important for the Registered Entity to perform the actions necessary to correct the issue as soon as possible in order to protect reliability and security of the BPS. This guide supplements information provided in Section 6.0 of Appendix 4C of the NERC ROP by providing further guidance on what should be included in mitigation.

The Registered Entity must retain evidence to provide proof of completion for all actions taken. For certain instances of noncompliance, the CEA will verify completion of each milestone. For the verification process, the Registered Entity will be required to submit evidence demonstrating completion to the ERO SEL. Regardless of whether verification occurs, it is best practice for the Registered Entity to upload evidence of completion each milestone to the ERO SEL.

Contents of Mitigation

What should be included in Mitigation submitted in Align?

All mitigation, both Mitigation Plans and mitigating activities, should include corrective actions to mitigate the noncompliance. These may include all controls and detective actions that will reduce the likelihood of a future occurrence and address the risk posed by the noncompliance and reduce or mitigate that risk, especially during the interim while implementing actions. The mitigation record is a part of the entire noncompliance record, so the Registered Entity should make sure the Self-Report, Finding Updates, and mitigation record contain all the information to understand the noncompliance. Registered Entities are strongly encouraged to take prompt steps to remediate noncompliance as soon as possible after discovery.

Mitigation should address each of the following:

[24] NERC only submits US jurisdiction Mitigation Plans to FERC.

1. Milestones that address Remediating Actions, Preventative Controls, Detective Controls, Corrective Controls, or other mitigating activities;[25]
    a. If an EOC analysis and cause analysis are not included in the Self-Report, the milestones should address these two areas;
2. Milestones and planned or actual completion dates for each; and
3. Interim Risk Reduction (required for Mitigation Plan).

Mitigation of the Noncompliance

This section provides a high-level summary of what should be included in the mitigation record. For detailed requirements of EOC, cause(s), and risk, refer to Chapters 1 and 2 above. Registered Entities should take prompt steps to address the noncompliance upon discovery.

Milestone Actions

Milestones should be relevant, measurable, and realistic for meeting the proposed completion date. Registered Entities are encouraged to have milestones to help both the CEA and the Registered Entity track progress. For each milestone, the Registered Entity should select the type of milestone task (*i.e.,* Remediating Action, Corrective Control, Preventative Control, Detective Control, and Other), include the milestone name, description of the milestone action, the planned completion date, and the actual completion date. The milestones should address distinct actions and should be descriptive. The mitigating activities must correct the issue, address the cause(s), and minimize the risk of recurrence. The Registered Entity should identify any EOC review and cause analysis performed as mitigating activities even if already completed. Note that the Registered Entity should complete EOC review prior to the completion of the cause analysis so the Registered Entity can analyze each of the issues discovered to determine if the causes are the same for all. The milestone should include any planned or completed activities that the Registered Entity will perform to mitigate the noncompliance.

Corrective and Remediating Actions or Controls

Registered Entities should design corrective and remediating actions or controls with the primary intent to remediate the noncompliance and restore compliance with the Reliability Standard as quickly as possible. Corrective actions or controls should also consider the cause and any other Reliability Standards impacted by the noncompliance. Remediating actions or controls should be considered the specific activities that remediated the noncompliance and brought the Registered Entity back into compliance with the Reliability Standard and Requirement. After determining the corrective and remediating actions or controls, the Registered Entity should ensure any undocumented knowledge (*e.g.*, something an employee knows and performs on a regular basis but is not documented) becomes documented, and training on updated and new procedures is provided to relevant personnel and new hires. The Registered Entity should document any training, including training materials, attendee list, *etc.*

Any actions that the Registered Entity completes prior to submittal of the mitigation, or that are in-progress as part of the initial reporting to the CEA, should also be included in this section.

Preventive and Detective Actions or Controls - Prevention of Recurrence

Registered Entities should implement preventive and detective actions or controls with the primary intent to detect potential recurrence of noncompliance in advance and to prevent it or reduce the likelihood of recurrence.

[25] The type of the mitigation milestone are defined as:
Corrective Control Action: Creation of an internal control designed to fix a problem that may arise.
Remediating Action: An action taken to return to compliance.
Preventive Control Action: Creation of an internal control designed to avoid an unintended event or consequence.
Detective Control Action: Creation of an internal control designed to identify errors or deviations from the norm.

When identifying these actions, the Registered Entity should focus on both procedural and technical controls that may be available to help detect and prevent future occurrences. Addressing the cause and any contributing factors with controls to prevent the likelihood of recurrence of the cause and contributing factors will generally lead to effective and sustainable mitigation. If a preventive control failed, the Registered Entity should evaluate why that previous control failed and what additional preventive controls it will implement.

Other Actions or Controls

If there are any other milestone actions that do not fit under Remediating, Corrective, Preventive, or Detective Actions, the Registered Entity should classify it as "Other" actions. These may include additional above and beyond steps the Registered Entity committed to take but may not necessarily fall directly under correcting or preventing the issue.

Completion Dates

For each milestone, the Registered Entity is required to provide a planned completion date. If the Registered Entity has completed the milestone activity, it should provide the actual completion date.

There are times when a planned completion date may need to be extended after the mitigation record has been accepted. Regarding Mitigation Plans, Section 6.5 of Appendix 4C of the NERC ROP states that at the CEA's discretion, the CEA may extend the completion deadline for a Mitigation Plan for good cause including, but not limited to:

1. Operational issues such as the inability to schedule an outage to complete a mitigation action; or
2. Construction requirements in the mitigation that require longer to complete than originally anticipated.

The Registered Entity must submit a request for an extension of any milestone or the completion date of the accepted mitigation record at least five business days before the original milestone planned completion date. The milestone extension request must include the new milestone planned completion date and the reason for the extension. This request must be submitted in Align, but the Registered Entity may also contact its CEA separately to discuss the request for extension. The CEA has the ability to accept or reject the proposed milestone extension request.

Extent of the Noncompliance

The Registered Entity should note any changes in the originally reported EOC of the noncompliance, which may require the submission of a Finding Update to the noncompliance. The Registered Entity may discuss the EOC review with the CEA to determine if a Finding Update is necessary. When identifying changes in the EOC of the noncompliance, the Registered Entity should consider all procedures, assets, facilities, or personnel that are involved or that could be impacted by the noncompliance and evidence to support the EOC determination.

The mitigation should include a narrative describing the comprehensive review by the Registered Entity to verify the full EOC of the noncompliance, which the CEA may review to determine how the Registered Entity performed the EOC.

Section ***Extent of the Noncompliance, if known*** in Chapter 1 provides in detail the information that should be included in the Mitigation Plan, mitigating activities, Self-Report, or Finding Update to address the full EOC.[26]

[26] In Align, the Registered Entity has the ability to notify the CEA if the EOC of the issue expanded as a result of the mitigation.

Additional Instances Identified During Mitigation

A Registered Entity is required to submit any additional instances of noncompliance that occur or are identified while implementing the mitigation activities. The Registered Entity should work with the CEA on how it should submit the information. Additional instances of noncompliance discovered during the implementation of the mitigation will not result in additional penalties or sanctions. This section is intended to encourage a Registered Entity to identify the EOC of a noncompliance in order to mitigate and remediate all instances—thereby preventing future instances.

Cause of the Noncompliance

The Registered Entity should also identify all cause(s) of the noncompliance when it submits the Self-Report. The mitigation milestones should address all the identified cause(s).

Section ***Causes of Noncompliance*** in Chapter 1 details the information that should be included in the Self-Report and updated as needed by submitting Finding Updates.

To ensure the Registered Entity properly addresses the cause, the Registered Entity should review its own compliance history to see if a same or similar issue or cause has occurred previously. This identification will provide information on the success of past mitigation. If the Registered Entity has multiple instances of noncompliance of the same or similar Reliability Standard/Requirement, there may be an underlying issue that the Registered Entity has not fully addressed.

Interim Risk Reduction

The Registered Entity must include steps that will reduce or eliminate risk to the BPS while it is implementing mitigation. The risk reduction steps must be specific for the risks identified. This step is especially critical for mitigation with longer durations. For formal Mitigation Plans, the Registered Entity must include the anticipated impact of the Mitigation Plan on the BPS reliability and an action plan to mitigate any increased risk to the reliability of the BPS while the Mitigation Plan is being implemented. It should include those steps that the Registered Entity has implemented and are in place to reduce or eliminate risk to the BPS. Based on the above considerations, actions and activities listed in the plan should include internal controls in place to mitigate the risk to the BPS.

Appendix A: Examples of Description, Scope, Cause, Risk, and Mitigation of Noncompliance

Quality self-reporting and mitigation consist not only of identifying the Reliability Standard and Requirement at issue, but also providing enough information to allow the CEA to understand the full description, scope, cause, and risk of the noncompliance, as well as what the Registered Entity (entity) is doing to correct and prevent the issue from recurring.

Reliability Standard - FAC-003-4 R2	Lacking	Acceptable
Description and Scope	The entity had an encroachment into the Minimum Vegetation Clearance Distance (MVCD) of a 230 kV line that led to a fault. The line tripped and reclosed as designed. A transmission line supervisor was dispatched to investigate the issue.	On July 20, 2017, at 2:20 p.m., the entity noted that there was a phase to ground fault that occurred on its 230 kV Point A to Point B line. The line tripped and reclosed as designed, avoiding a Sustained Outage. A transmission line supervisor was dispatched to investigate the issue. Prior to the supervisor being able to see the location of the fault, the ground crew needed to go in and clear a path due to the surrounding undergrowth vegetation. When the transmission line supervisor arrived at the site, it was noted that there was some evidence of burning on a poplar located near the line. It was determined that the entity, as a Transmission Owner, was in violation of FAC-003-4 R2 for having an encroachment due to vegetation growth into the line MVCD. After investigating the site, the supervisor ordered vegetation removal to take down the tree and ordered a review of all vegetation management records for the line.
Cause	The entity noted the cause of the noncompliance was related to an error in the Spring aerial inspection log.	The entity determined the cause of the noncompliance related to an error in documentation of the aerial inspection log. The contractor did perform an aerial inspection in the Spring but failed to note that part of the line needed a ground inspection to determine the vegetation distance from the line due to other undergrowth vegetation making the distance difficult to determine. A review of current procedures for aerial inspection logs showed that there were no distinctions within the logs for elements inspected from the air and had no issues and any that may require follow up. Normal procedure was to include a comment as needed. This was assessed to be a gap in controls within the procedure and documentation to include clear options for “inspected and complete” and “inspected but not complete”.
Risk Assessment	The risk was mitigated because the line tripped and reclosed as designed, which resulted in no customer outages. There were no Interconnection Reliability Operating Limits (IROL) or System Operating Limits (SOL) exceedances.	The violation posed a moderate risk to the reliability of the bulk power system. Improper vegetation management that causes an unplanned, Sustained Outage could result in higher risk system conditions or loss of load. The likelihood of the impact was reduced because the line tripped and reclosed as designed, which resulted in a momentary outage. Automatic reclosing operated as designed, restoring the line to service in five seconds, limiting any impact to the 230 kV system. This line was neither an element of an IROL nor an element of a Major WECC Transfer Path. In addition, the momentary loss of the line did not result in an exceedance of any SOLs. The line was loaded at

Reliability Standard - FAC-003-4 R2	Lacking	Acceptable
		20% at the time of the fault and nearby facilities operated within normal ratings. Further, in the event of a Sustained Outage, the entity was able to demonstrate Operating Plans that would have mitigated operating above the normal ratings of their facilities. Due to the identified gap in controls, it is possible that other instances whereby a line was inspected but additional ground inspection was required. Prior documentation showed this gap only to exist in inspection logs beginning in 2017; thereby limiting the scope of the identified gap.
Mitigation	To mitigate this issue, the entity: 1) trimmed the tree; 2) discussed the issue with the transmission line supervisor and the arbor contractor; and 3) conducted refresher trainings with affected employees on the FAC-003 procedures.	To mitigate this issue, the entity: 1) removed the tree; 2) conducted a review of all vegetation management records on the line; 3) after identifying the error related to aerial records, conducted a review of all the aerial contractor's work to see if there were any other concerns that needed to have ground inspections; 4) conducted a foot patrol inspection of the remainder of the line to see if there were any other concerns; 5) confirmed that the line would have the aerial as well as ground inspection for both Spring and Fall inspections; 6) updated procedures to require ground inspection for all lines and that the contractor needs to note all vegetation conditions; 7) updated its technical specifications related to reporting of vegetation conditions and its inspection practices. This includes the addition of a documented sign-off process; 8) installed software that accommodates planning and implementation of annual work performance, schedules, work orders, work in progress, and reporting capabilities; and 9) added an annual training requirement for a review of the FAC-003 procedures.

Reliability Standard - VAR-002-4 R3	Lacking	Acceptable
Description and Scope	On July 1, 2016, at 2:42 p.m., the entity experienced an issue with its system and the automatic voltage regulator (AVR) switched to manual mode. The AVR alarm activated, and the operator was aware of the alarm but failed to recognize that the AVR status changed to manual mode and therefore did not notify the Transmission Operator (TOP) of the status change within the required 30 minutes.	On July 22, 2016, the entity submitted a Self-Report stating that, as a Generator Operator, it had a possible noncompliance with VAR-002-4 R3. The entity failed to notify its associated TOP of the status change of the AVR within 30 minutes of the change in one instance. On July 1, 2016, at 2:42 p.m., the entity's generator AVR switched to manual mode. The operator noticed and acknowledged the AVR alarm but failed to recognize that the AVR status changed to manual mode and required notifying the TOP of an AVR status change within 30 minutes. The operator had to adjust the voltage manually to maintain the assigned schedule. While the operator was adjusting the voltage to maintain the voltage schedule, a technician that was supporting the operator recognized that the AVR was in manual mode. Upon recognizing the AVR was no longer in automatic mode, the operator returned the AVR to automatic and then notified the TOP of the change in status at 3:32 p.m. The entity determined it was noncompliant July 1, 2016, from 3:12 p.m. (when the entity should have notified the TOP that the AVR status changed to manual mode) until 3:32 p.m. when the entity returned the AVR to automatic mode and notified the TOP of the generator unit's status.
Cause	The cause was human error by the operator.	The cause was a lack of operator awareness that caused the incorrect identification and clearing of the AVR alarm. The operator had reduced awareness regarding this issue as a result of infrequent AVR status alarm activations, coupled with a history of other more frequent alarm activations that the entity previously cleared without incident. Following a review of operator documented procedures and operator interviews, it was determined that operator acknowledgement of a change to AVR status was done by clearing the alarm and that a distinct operator acknowledgement of the AVR status change was not documented. An additional review of training programs indicate that operators are not provided clear guidance on how to ensure an AVR status change is consistently acknowledged.

Reliability Standard - VAR-002-4 R3	Lacking	Acceptable
Risk Assessment	The risk was reduced by the operator monitoring the voltage and maintaining the proper voltage per the schedule. Additionally, the unit did not trip during this time, so no harm occurred.	The failure to notify the TOP of a change in the status of a generator AVR reduces the TOP's situational awareness and increases the potential that online generators will be less capable of responding to voltage excursions during system events. The risk was reduced as the operator was monitoring the voltage and maintaining the proper voltage schedule by making manual adjustments. During this 20-minute timeframe, the unit did not trip and there was no loss of load. Additionally, the unit has a nameplate rating of 143.9 MVA, and its associated substation is not part of an Interconnection Reliability Operating Limit. Lastly, the entity had other knowledgeable staff that led to the technician immediately recognizing the AVR status was not correct, resulting in prompt reporting to the operator and to the TOP.
Mitigation	To mitigate this issue, the entity: 1) returned the AVR to automatic mode and notified the TOP; 2) updated signage at the operator station to better explain the meaning of the AVR alarm; and 3) held a refresher training on its procedures with the operator.	To mitigate this issue, the entity: 1) returned the AVR to automatic mode and notified the TOP; 2) added a message to the operator's screen that requires acknowledgement from the operator to ensure they check whether the AVR status changed and, if it did, includes a reminder that the TOP needs to be notified; 3) reviewed the procedures and updated the narrative around the meaning of the alarms and what actions need to be taken by the operator; 4) conducted a training on the revised procedures with all of the operators and added the training to the annual training classes; 5) conducted a review of all AVR alarm logs in the past year and compared against the TOP notification. The review did not uncover any other instances; and 6) held a mandatory lessons learned meeting to discuss this issue with the operators at each of its facilities.

Reliability Standard - PRC-005-6 R3	Lacking	Acceptable
Description and Scope	The entity did not have evidence of the four-month maintenance for its batteries per the intervals in the PRC-005-6 R3 tables. The entity discovered it missed the maintenance during a review and performed testing two days after the review.	On September 25, 2017, the entity submitted a Self-Report stating that, as a Transmission Owner, it had a possible noncompliance with PRC-005-6 R3. The entity failed to maintain its batteries per the time-based maintenance program. On August 1, 2017, the entity conducted a review of its battery maintenance and testing records and discovered it failed to have evidence of the four-month maintenance and testing for 15% of its total Valve Regulated Lead-Acid batteries. The batteries supply Protection System relays on two 138 kV lines. According to the entity's records, the entity last tested the batteries on February 8, 2017, and should have maintained and tested the batteries by June 8, 2017. On August 3, 2017, the entity performed the maintenance and testing and found no issues with the batteries. The entity plans on conducting a review of its maintenance and testing records at its two other facilities in October 2017.
Cause	The cause of the noncompliance was the individual response responsible for the maintenance failed to follow maintenance procedures and appropriately schedule the maintenance and testing.	The cause was that the individual responsible for performing the maintenance and testing on these devices dismissed the calendar alert when beginning the maintenance and was then interrupted during the review and failed to finish the review. Further, there was a lack of management oversight and internal controls to periodically review or verify that the entity's maintenance and testing program was being performed as scheduled.
Risk Assessment	The risk was reduced as the batteries only missed one quarterly inspection and, when testing occurred, the batteries were within parameters.	The failure to maintain batteries could lead to misoperation of the Protection Systems on the two 138 kV lines. The likelihood of a misoperation was reduced as the entity had alarms in place that would have alerted operators if the batteries did not operate as intended. In addition, the entity had backup batteries that were tested at the appropriate interval. The batteries at issue had been tested regularly prior to the missed interval. The batteries only missed one inspection and, when testing occurred, the batteries were within parameters. Finally, the entity did not experience a loss of load, generation, or transmission elements, system disturbances, Protection System operations or Misoperations, or BES emergency conditions prior to, during, or as a result of the missed interval.

Reliability Standard - PRC-005-6 R3	Lacking	Acceptable
Mitigation	To mitigate this issue, the entity: 1) completed the missed battery maintenance; 2) revised the Protection System Maintenance and Testing Program to include appropriate responsibilities for the maintenance; and 3) completed an inventory of the PRC-005 related Protection System devices to ensure that all components have been identified.	To mitigate this issue, the entity: 1) completed the missed battery maintenance in accordance with table 1-4 of PRC-005-6; 2) verified the previous maintenance and testing completion dates were performed in accordance with the intervals set forth in the PRC-005-6 tables; and 3) performed any maintenance or testing that had exceeded an interval identified in Step 2 and notified the CEA. To prevent recurrence of the issue, the entity: 1) updated the tracking software notifications to include management of required maintenance and testing intervals; 2) updated the tracking software so it linked with the scheduling software to ensure all maintenance days are captured automatically in the scheduler; 3) updated the documented process to require acknowledgement of scheduled maintenance and testing only after the completion and update of the results in the system; and 4) management created a new process to periodically review the results of the entity's maintenance and testing program with the tracking and scheduling software data.

Reliability Standard - CIP-004-6 R4	Lacking	Acceptable
Description and Scope	The entity submitted a Self-Report indicating it was in violation of CIP-004-6 R4. A contractor needed access to a Physical Access Control System (PACS) to perform new responsibilities as they were moving systems from one security management software to another. The system administrator noted that the contractor had full access to the old system, so the system administrator granted access privileges to the new system.	On March 24, 2018, the entity submitted a Self-Report indicating that as a Generator Owner and Generator Operator, it was in violation of CIP-004-6 R4. On February 18, 2017, during a routine review of the system, a system administrator discovered a contractor's access in a PACS (security management software) was incorrect. Specifically, on February 2, 2017, the system administrator changed a physical security contractor's access privileges for a security management software tool without having documentation of proper authorization. At the time of the noncompliance, the entity was in the process of migrating from one security management software tool (Tool A) to another (Tool B). The contractor already had read-only access to the Tool A security management software tool, and had authorized NERC CIP electronic access to the Tool B security management software. The contractor was working with entity staff who were testing Physical Security Perimeter (PSP) access points and needed the Tool A security management software access that would allow him to monitor badge activity at the PSP doors. The contractor was not aware that the change in access privileges for the Tool A security management software would require additional authorization, so the contractor went directly to a system administrator to request access to the screens that would allow the contractor to view the badge activity. The system administrator was aware that the contractor had full access in the Tool B security management software, but was not aware that the contractor did not have documented authorization for the same type of access in the Tool A security management software. The system administrator granted full access to the Tool A security management software tool when the contractor only was authorized for read-only access on the Tool A security management software tool. The issue began on February 2, 2017, when the system administrator granted full access to the Tool A security management software tool for a contractor without proper authorization, and ended on September 20, 2017, when the entity removed the unauthorized access privileges.

Reliability Standard - CIP-004-6 R4	Lacking	Acceptable
Cause	The cause was a failure to ensure the access management program procedure was followed and the authorization request was properly processed.	The cause was that the entity did not have a robust access management program procedure in place to deal with changes that may occur due to system modifications. Specifically, changes in access privileges in the access management program procedure were not well enough defined to require additional authorization. Additionally, the entity had not implemented an internal control preventing and/or detecting the system administrator granting access without proper authorization.
Risk Assessment	The risk was reduced because the contractor had a valid Personnel Risk Assessment, completed the cyber security training, and was in good standing with the company. Additionally, the contractor had authorized read-only electronic access to the old system and had authorized full electronic access on the new system.	The risk was reduced because the contractor had a valid Personnel Risk Assessment, completed the cyber security training, and was in good standing with the company. Additionally, the contractor had authorized read-only electronic access to the old security management software tool and had authorized electronic access on the new security management software tool. The entity had other security measures in place to limit access to authorized personnel, including 24/7 surveillance. The PACS have additional controls, including account/password management, security event monitoring, patching, malware prevention, change management, restricted ports/services, incident response procedures, and recovery procedures. Additionally, the entity sends the audit logs to an offsite security information event monitoring system for further analysis. Finally, the entity implemented a backup process for deactivating physical and electronic access.

Reliability Standard - CIP-004-6 R4	Lacking	Acceptable
Mitigation	To mitigate this issue, the entity: 1) removed the contractor's unauthorized electronic access to the new system; and 2) held a lessons learned meeting with the system administrators to review the noncompliance.	To mitigate this issue, the entity: 1) removed the contractor's unauthorized electronic access to the old security management software tool; 2) renamed the user roles within the PACS that require NERC CIP authorization; 3) held a lessons learned meeting with the system administrators to review the noncompliance and to reinforce the importance of following the access management program to make sure all requests are submitted and approved properly; 4) held a lessons learned with the contractor and employer to not circumvent the approval process. In addition, verbiage was added to training given to contractors to reflect this and sent to all vendor companies; 5) revised the access management program procedure to include a checklist for the system administrators to complete prior to changing access privileges; this includes adding dates and a signed approval around the authorization request and approval process; and 6) conducted training on the revised access management program procedure and added this training to the annual training for staff.

Reliability Standard - CIP-010-2 R1	Lacking	Acceptable
Description and Scope	While conducting an internal review, the entity discovered a discrepancy between the baseline configuration and the devices' running configuration. The entity submitted a Self-Report stating it was in violation of CIP-010-2 R1 for failing to document seven workstation baselines, as required under CIP-010-2 R1.	On June 2, 2018, while conducting an internal review, the entity discovered a discrepancy between the baseline configuration and the running configuration on seven newly installed BES Cyber Assets workstations included in a high impact BCS. During the investigation into this issue, the entity determined that on April 1, 2018, when it deployed the BES Cyber Assets, it did not document all of the ports on the baseline configuration. Specifically, the entity discovered that it failed to document all the ports on the seven newly installed workstations to its baseline configuration tool, as required under CIP-010-2 Requirement R1, Part 1.1.
Cause	The cause was an inadequate process around baseline configurations.	The cause was an insufficient change management process to properly document applicable Cyber Asset baselines. Specifically, the entity lacked a documented process to ensure its personnel properly documented necessary baseline elements for applicable Cyber Assets. Additionally, the entity did not implement internal controls to prevent or detect the failure to document baseline configurations for newly installed assets.
Risk Assessment	The risk was reduced because the workstations are located inside an Electronic Security Perimeter (ESP) and are protected by firewall(s), which control access to the ESP systems, as well as additional layers of firewalls specific to the workstations network, restricting any unauthorized access to the BES Cyber Systems.	The entity's insufficient change management process and undocumented Cyber Asset baselines elements could lead to improper management of Cyber Assets. Improper management of Cyber Assets baselines may increase the likelihood of a threat exploitation by malicious actors. The risk was reduced because the entity had multiple controls in place to prevent the likelihood of the potential impact. First, the workstations at issue were physically located within a PSP. Second, the workstations were logically located inside an ESP. Third, the workstations were on a separate section of the network separated by virtual local area networks. Finally, the entity possessed a number of additional controls, including automated security information event monitoring systems, intrusion detection systems, and antivirus software. Throughout the violation period, these controls did not detect any anomalies, malicious traffic, or malicious code. The entity confirmed that during the period at issue, there were no changes to the seven workstations that would have resulted in a deviation to the baseline, and the entity did not have any Reportable Cyber Security Incidents during the violation duration.

Reliability Standard - CIP-010-2 R1	Lacking	Acceptable
Mitigation	To mitigate this issue, the entity: 1) conducted a review of all applicable Cyber Assets to determine if there were any other discrepancies between the baseline configuration and the running configuration; and 2) completed the baseline configuration for the workstations.	To mitigate this issue, the entity: 1) completed the baseline configuration for the seven workstations; 2) conducted extent of conditions to all business units to verify this issue did not take place elsewhere; 3) enhanced the entity's change management and new project processes to improve compliance involvement and oversight of project development activities, including directly assigning compliance staff to applicable project development teams; 4) revised the process document for building new Cyber Assets; 5) revised the technical architecture documents to include a decision tree for the project to evaluate Cyber Assets and determine applicability to NERC CIP Standards; 6) modified the documented processes for new Cyber Assets, to include explicit guidelines for identifying all NERC Cyber Assets during the new build process; 7) revised the applicable new build workflow processes in the tool to preclude closing new build requests until all applicable baseline activities are performed; 8) conducted additional training on the revised new build processes, the other process changes made as part of the mitigation of this issue, and the requirement to perform baseline activities on new NERC Cyber Assets; and 9) conducted a review of all applicable Cyber Assets to determine if there were any other discrepancies between the baseline configuration and the running configuration.

Reliability Standard - CIP-007-6 R2	Lacking	Acceptable
Description and Scope	The entity failed to evaluate 18 security patches within 35 days of being released. The patches were released on June 7, 2017, and the entity performed the evaluation on July 29, 2017.	On August 13, 2017, the entity submitted a Self-Report indicating that, as a Generator Owner, Generator Operator, Transmission Owner, and Transmission Operator, it was in violation of CIP-007-6 R2. Specifically, the entity failed to perform an evaluation on 18 security patches that were applicable to its Medium Impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) within 35 days of the patches being released. On May 12, 2017, the entity's remote security scanning tool experienced an issue which caused it to stop scanning for and downloading patches from a single monitored source identified in the entity's patch management process. As a result, the entity failed to monitor the patch source for 18 patches released on June 7, 2017. As such, the entity should have performed the required evaluation of these patches by July 12, 2017. On July 28, 2017, the entity discovered the issue during a review of reports from its configuration management tool and performed the required evaluation of the 18 patches in question. The entity performed the required evaluation on July 29, 2017. The security patches were primarily for addressing a vulnerability with internet browsing and when the entity performed the evaluation and when the entity assessed the patches it was determined the patches had a vulnerability risk rating of zero. The duration of the issue was July 13, 2017 (the day after the entity should have performed the evaluations of the first security patches at issue) to July 29, 2017 (the date the entity performed the required evaluation of all 18 applicable security patches).
Cause	The cause was a failure to follow the patch management program.	The cause was the entity did not have a well-defined process to detect and address issues with its remote security scanning tool. In particular, the entity lacked a process to actively monitor its remote security scanning system to ensure the system was identifying all patches from the entity's monitored source list, as well as a process to verify that the patches requiring evaluations have been properly identified by the remote security scanning tool.

Reliability Standard - CIP-007-6 R2	Lacking	Acceptable
Risk Assessment	The risk was reduced because when the entity evaluated the patches, there were no issues, and the devices are located in the supervisory control and data acquisition systems within the PSP.	Failure to perform security patch assessments in a timely manner could result in an attacker gaining access to the entity's BES Cyber Systems to cause disruptions to its operating capabilities, thereby affecting the reliability of the Bulk Power System (BPS). The risk was reduced for several reasons. The duration of the issue was short, only lasting 16 days. The patches at issue addressed a vulnerability that would typically be exploited through internet access. Because the workstations missing the patches had no internet access, there was a reduced likelihood that an external or non-trusted source could have exploited this vulnerability on the impacted workstations. When the entity performed the evaluation and assessed the patches, it was determined the patches had a vulnerability risk rating of zero. Additionally, the entity uses an intrusion protection system that protects all critical environments including the ones at issue here, as well as security zones defined by access privilege/application data communication to segregate systems and firewalls. Finally, the entity monitors all of the devices at issue on a continuous basis for unauthorized intrusions and configuration changes and did not detect any unauthorized activity on these devices during the duration of the patching issue.
Mitigation	To mitigate the issue, the entity: 1) performed an evaluation of the patches missed during the period in question; and 2) installed all applicable patches.	To mitigate the issue, the entity: 1) performed an evaluation of the patches missed during the period in question; 2) installed all applicable patches; 3) deployed systems to monitor its remote security scanning tool to detect issues and provide alerts to the entity personnel; 4) updated its patch management process to require entity personnel to verify that the remote security scanning tool has identified applicable patches prior to performing patch evaluations; 5) provided the updated patch management process to affected entity personnel; 6) trained affected entity personnel on the updated process and added this to the new hire training and annual training classes; and 7) completed a review of all patches released in the last year to confirm no other patches missed the deadline and confirm the entity did not find any other missed patch evaluations.

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 an internal compliance program (*e.g.*, internal controls)?
    - 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 function and 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)?
    - Was it discovered during the implementation of mitigating activities for an open enforcement action? The Registered Entity could discuss with the CEA if it should submit a Finding Update to the open enforcement action or if it should submit a new Self-Report.
    - Was it revealed through an event or other operational occurrence?
  - What date did the Registered Entity discover the noncompliance? If discovered due to an event, provide the date of that event and, if applicable, the category of the event.
  - 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 and does the description related back to the language and content in the Reliability Standard/Requirement? If the noncompliance started under a previous version of the Reliability Standard and Requirement, the Registered Entity can provide that information in the detailed description.
  - 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 EOC review been performed, and if so, what other processes, procedures, controls, assets, facilities, or personnel were impacted or could be impacted by the noncompliance? The CEA and NERC should be able to understand how the Registered Entity determined that the level of EOC review was appropriate. The Registered Entity should include how the EOC was performed (e.g., automated tools, manual reviews, sampling) and what evidence the Registered Entity reviewed. The Registered Entity may discuss the level of EOC review that is appropriate with the CEA.

- Does the Self-Report describe the cause of the noncompliance?
  - Has the cause(s) 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?

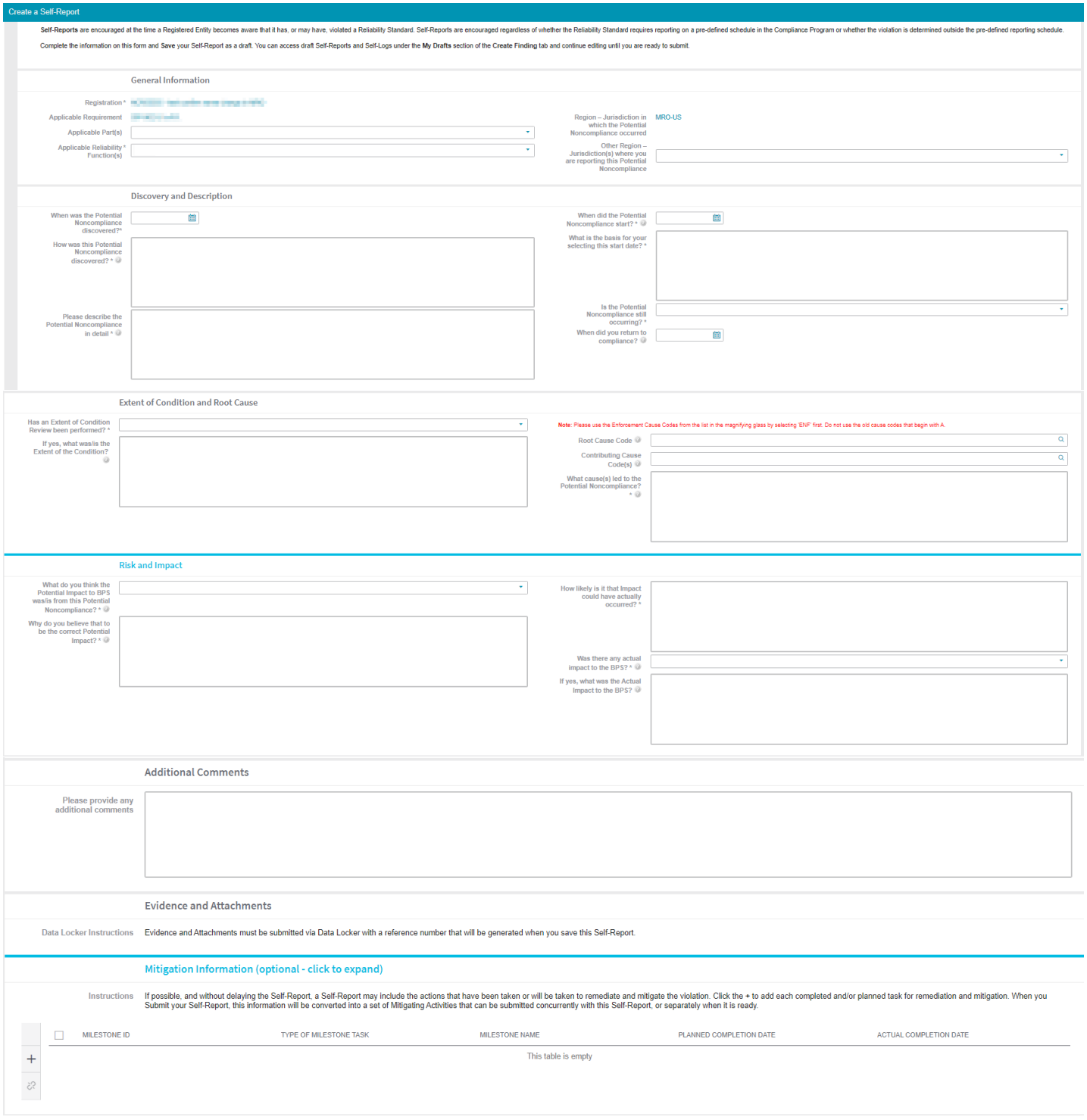
- Does the Self-Report include duration information?
  - What date did the noncompliance start? What date did the noncompliance end? Include an explanation for those dates, if known. The end date is when the Registered Entity corrected the noncompliance (*i.e.*, remediated), which is not necessarily the mitigation completion date.

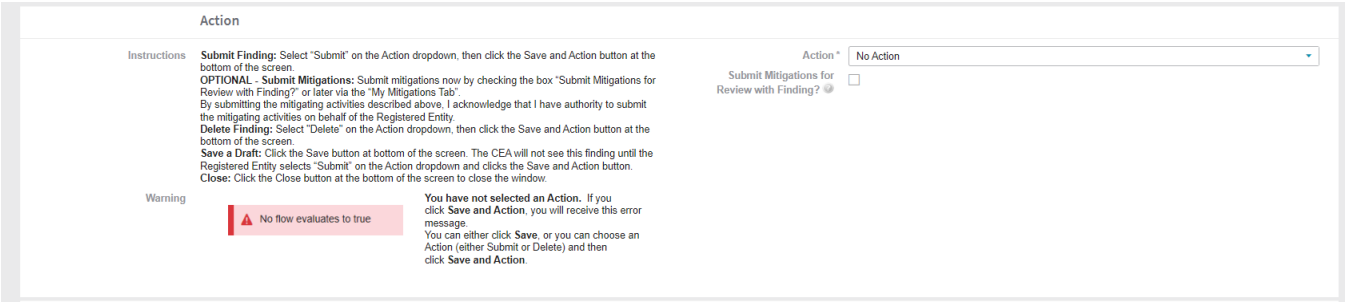
- Does the Self-Report address the risk to both the BPS and the Registered Entity associated with the noncompliance?
  - What were the system conditions during the event? For example, did the noncompliance take place while the system was stressed (*i.e*., during an Energy Emergency or when other emergency or special operating procedures were in effect)?
    - The system conditions at the time of the issue, *i.e.*, N-1, Misoperations, extreme weather, and any extenuating circumstances.
  - Was there any potential for loss of a Protection System device, degradation or loss of a BES element, loss of a BCS or information, or providing unauthorized access to BCSs?
  - What are the size, nature, criticality, and location of the facilities at issue?
  - What actual impact occurred, what potential impact could have occurred, and what was the likelihood of the potential impact occurring?
    - Was the cause of the noncompliance the same as or similar to prior instances of noncompliance?
    - Were the circumstances surrounding the noncompliance rare or common?
    - What remediation steps are already in place to address the issue?
    - What controls will the Registered Entity put into place to reasonably prevent recurrence?
    - Were the controls implemented Registered Entity-wide?
    - Were the controls business-function or process driven? Each business function may have different controls in place that may help detect or prevent issues.
  - How many assets were at issue and what was the nature and function of the asset(s) (*e.g*., the affected assets were a High Impact BCA and a Medium Impact PACS)? Does the affected asset(s) perform a reliability task?
  - What other systems, facilities, or staff are exposed to the same possible failure modes?
  - Were there any Misoperations or exceedances of system operating limits or IROL during the course of the noncompliance?
  - Was there potential to affect any CIP technical controls that may have impacted BCSs?
  - The time horizon of the noncompliance, *i.e.*, did the noncompliance impair or threaten real-time operations or day-ahead operations planning?
  - Was the noncompliance isolated or a systemic/general control failure potentially impacting multiple processes/systems.

- If the Registered Entity has sensitive information, the Registered Entity should upload that information into the ERO SEL instead of including it in the Self-Report form in Align.

Appendix C: Self-Report Align Form

The images below provide a quick view of the Self-Report form that a Registered Entity will complete in Align.




Action
Instructions
Submit Finding: Select "Submit" on the Action dropdown, then click the Save and Action button at the bottom of the screen.
OPTIONAL - Submit Mitigations: Submit mitigations now by checking the box "Submit Mitigations for Review with Finding?" or later via the "My Mitigations Tab".
By submitting the mitigating activities described above, I acknowledge that I have authority to submit the mitigating activities on behalf of the Registered Entity.
Delete Finding: Select "Delete" on the Action dropdown, then click the Save and Action button at the bottom of the screen.
Save a Draft: Click the Save button at bottom of the screen. The CEA will not see this finding until the Registered Entity selects "Submit" on the Action dropdown and clicks the Save and Action button.
Close: Click the Close button at the bottom of the screen to close the window.
Action *
No Action
Submit Mitigations for Review with Finding?
Warning
No flow evaluates to true
You have not selected an Action. If you click Save and Action, you will receive this error message.
You can either click Save, or you can choose an Action (either Submit or Delete) and then click Save and Action.

Appendix D: Mitigation Checklist

The intent of this checklist is to provide a quick outline of the topics discussed in ***Chapter 3: Mitigation.***

- Identify the Registered Entity contact.
  - If the CEA requests a formal Mitigation Plan, is a Registered Entity contact specified?
- The mitigation should include a narrative describing the comprehensive review by the Registered Entity to verify the full EOC of the noncompliance, which the CEA may review to determine how the Registered Entity performed the EOC. Describe the EOC of the noncompliance being mitigated.
  - Has the EOC changed from what was originally reported (*e.g.*, additional devices/facilities/personnel found to be in scope)? Did the Registered Entity consider all procedures, assets, facilities, or personnel that were directly impacted or could be impacted by the noncompliance?
- The mitigation milestones should address all the identified cause(s). Addressing the cause and any contributing factors with controls to prevent the likelihood of recurrence of the cause and contributing factors will generally lead to effective and sustainable mitigation.
  - Has the cause(s) been completely identified?
  - Were there any other contributing causes?
  - If the noncompliance was not discovered by the Registered Entity, did the Registered Entity review its detective processes to determine if anything needs to be improved or implemented?
  - Has the Registered Entity reviewed its own compliance history to see if a same or similar issue has occurred previously?
- Include all corrective, remediating, detective, and prevention actions or controls to address the current issue and prevent recurrence.
  - Do the actions relate to Standard and Requirement in scope?
  - Do the actions address the cause(s) of the noncompliance?
  - What is being mitigated?
  - How is it being mitigated?
  - When is it being mitigated?
  - Has prevention of recurrence been addressed?
  - Have all actions taken to resolve the noncompliance and reasonably prevent recurrence been included?
  - Have completion dates for all actions completed prior to submission of the plan been included?
- Milestones should be relevant, measurable, and realistic for meeting the proposed completion date. Registered Entities are encouraged to have milestones to help both the CEA and the Registered Entity track progress. Ensure that milestones address distinct actions and are descriptive. The milestones should address the full scope and all instances of noncompliance.
  - Have milestones been defined where appropriate?
    - Does each milestone include sufficient detail?
    - Are the milestone intervals reasonable?
    - Are the milestone intervals no longer than three months apart?
  - Remember to retain evidence to provide proof of completion for all actions taken. For certain instances of noncompliance, the CEA will verify completion of each milestone. For the verification process, the Registered Entity will be required to submit evidence demonstrating completion to the ERO SEL. Regardless of whether verification occurs, it is best practice for the Registered Entity to upload evidence of completion each milestone to the ERO SEL.
- For each milestone, the Registered Entity is required to provide a planned completion date. If the Registered Entity has completed the milestone activity, it should provide the actual completion date.

  - Verify that all milestones will be complete by the overall proposed plan completion date of the mitigation record.
  - There are times when a planned completion date may need to be extended after the mitigation record has been accepted. The Registered Entity must submit a request for an extension of any milestone or the completion date of the accepted mitigation record at least five business days before the original milestone planned completion date. The milestone extension request must include the new milestone planned completion date and the reason for the extension.

- Describe the interim risk to the reliability of the BPS while the mitigation is being implemented. The Registered Entity must include steps that will reduce or eliminate risk to the BPS while it is implementing mitigation.
  - Does the mitigation contain interim steps to address this risk? The risk reduction steps must be specific for the risks identified.

- Describe the prevention of future risk to the reliability and security of the BPS. Registered Entities should implement preventive and detective actions or controls with the primary intent to detect potential recurrence of noncompliance in advance and to prevent it or reduce the likelihood of recurrence.
  - How will the successful completion of this mitigation prevent or minimize the probability that the Registered Entity incurs further risk of noncompliance with the same or similar Reliability Standards requirements in the future?

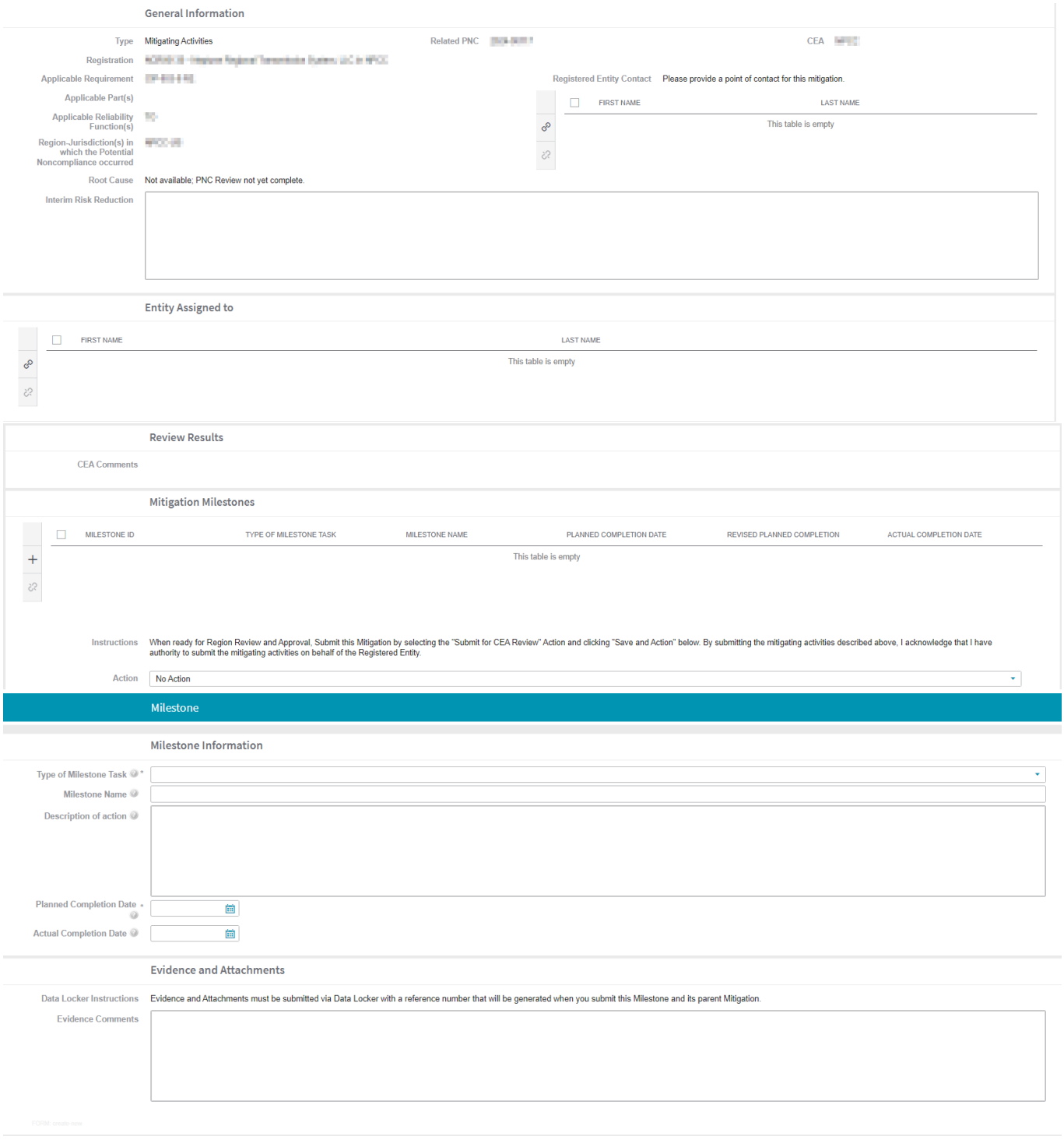
- Describe how the mitigation actions will reduce the likelihood of recurrence.
  - If the Registered Entity had prior instances of noncompliance, does the mitigation address how the current noncompliance differs (or does not differ) from previous instances?
  - Does the mitigation address how the specific enumerated action will help to prevent recurrence?

- A Registered Entity is required to submit any additional instances of noncompliance that occur or are identified while implementing the mitigation activities. The Registered Entity should work with the CEA on how it should submit the information.

- If the Registered Entity has sensitive information, the Registered Entity should upload that information into the ERO SEL instead of including it in the Self-Report form in Align.

Appendix E: Mitigation Align Form

The images below provide a quick view of the Mitigation form that a Registered Entity will complete in Align.



Appendix F: Reference Documents

FERC Guidance or Reference Documents

- *North American Electric Reliability Corporation,* 161 FERC ¶ 61,187 (2017) (January 2019 RAI Order on Compliance Filing) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/LetterOrder_AnnualCE-FFT_Program_20190124.pdf
- *North American Electric Reliability Corporation,* 161 FERC ¶ 61,187 (2017) (November 2017 RAI Order on Compliance Filing) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20on%20CMEP.pdf
- *North American Electric Reliability Corporation,* 153 FERC ¶ 61,130 (2015) (November 2015 RAI Order on Compliance Filing) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_CMEP_20151104_RR15-2.pdf
- *North American Electric Reliability Corporation,* 153 FERC ¶ 61,024 (2015) (October 2015 Risk Based Registration Initiative Order on Compliance Filing) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_10152015_RR15-4.pdf
- *North American Electric Reliability Corporation,* 150 FERC ¶ 61,213 (2015) (March 2015 Risk Based Registration Initiative Order) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_20150319_RR15-4.pdf
- *North American Electric Reliability Corporation,* 150 FERC ¶ 61,108 (2015) (February 2015 RAI Order) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_CMEP_20150219_RR15-2.pdf
- *North American Electric Reliability Corporation,* 148 FERC ¶ 61,214 (2014) (September 2014 FFT Compliance Filing Order) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/FFT_Order_RC11-6-004_20140918.pdf
- *North American Electric Reliability Corporation,* 143 FERC ¶ 61,253 (2013) (June 2013 FFT Compliance Filing Order) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_CEI-FFT_20130620_RC11-6-004.pdf
- *North American Electric Reliability Corporation,* 139 FERC ¶ 61,168 (2012) (March 2012 FFT Rehearing Order) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_Clarification_FFT_March2012_20120531.pdf
- *North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) (March 2012 FFT Order) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/OrderConditionallyAcceptingNewEnfocementMechFiling_031512.pdf
- *North American Electric Reliability Corporation*, 134 FERC ¶ 61,209 (2011) (Turlock Order) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_Review_Notice_Penalty_3.17.11.pdf
- *Enforcement of Statutes, Orders, Rules, and Regulations*, 132 FERC ¶ 61,216 (2010) (Revised Policy Statement on Penalty Guidelines) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/RevisedPolicyStatementOnPenaltyGuidelines_20100917.pdf
- Further Guidance Order on Filing Reliability Notices of Penalty, 129 FERC ¶ 61,069 (2009) http://www.nerc.com/files/Further%20guidance%20order%2020091026-3041(22732912).pdf
- *Guidance Order on Reliability Notices of Penalty,* 124 FERC ¶ 61,015 (2008) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/NoticeOfPenaltyOrder.pdf

- *Policy Statement on Compliance*, 125 FERC ¶ 61,058 (2008) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/PolicyStatementOnCompliance-10162008.pdf
- *Revised Policy Statement on Enforcement*, 123 FERC ¶ 61,156 (2008) https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/PL08-3-000_RevisedPolicyStatementOrder_05152008.pdf
- FERC Overall Approach to Root Cause Analysis https://www.ferc.gov/industries-data/hydropower/dam-safety-and-inspections/taum-sauk-pumped-storage-project-p-2277-dam
- Department of Energy Root Cause Analysis Guidance Document https://www.standards.doe.gov/standards-documents/1000/1104-std-1992

NERC Guidance or Reference Documents

- Cause Analysis Methods for NERC, Regional Entities, and Registered Entities, issued September 2011 https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/Cause%20Analysis%20Methods%20for%20NERC,%20Regional%20Entities,%20and%20Registered%20Entities_09202011_rev1.pdf
- NERC Rules of Procedure http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
- NERC Enforcement Filings and Templates http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx
- NERC Align and Secure Evidence Locker https://www.nerc.com/ResourceCenter/Pages/Align-SEL.aspx
- NERC Risk-Based CMEP http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx
- NERC Event Analysis Program https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
- NERC Standards https://www.nerc.com/pa/Stand/Pages/default.aspx
- ERO Enterprise Guide for Internal Controls http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf
- ERO Enterprise Guide for the Multi-Region Registered Entity Coordinated Oversight Program https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Coord_Oversight_Guide.pdf