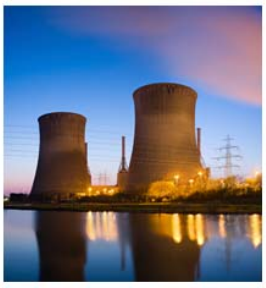
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Registered Entity Self-Report and Mitigation Plan User Guide

June 2018

RELIABILITY | ACCOUNTABILITY

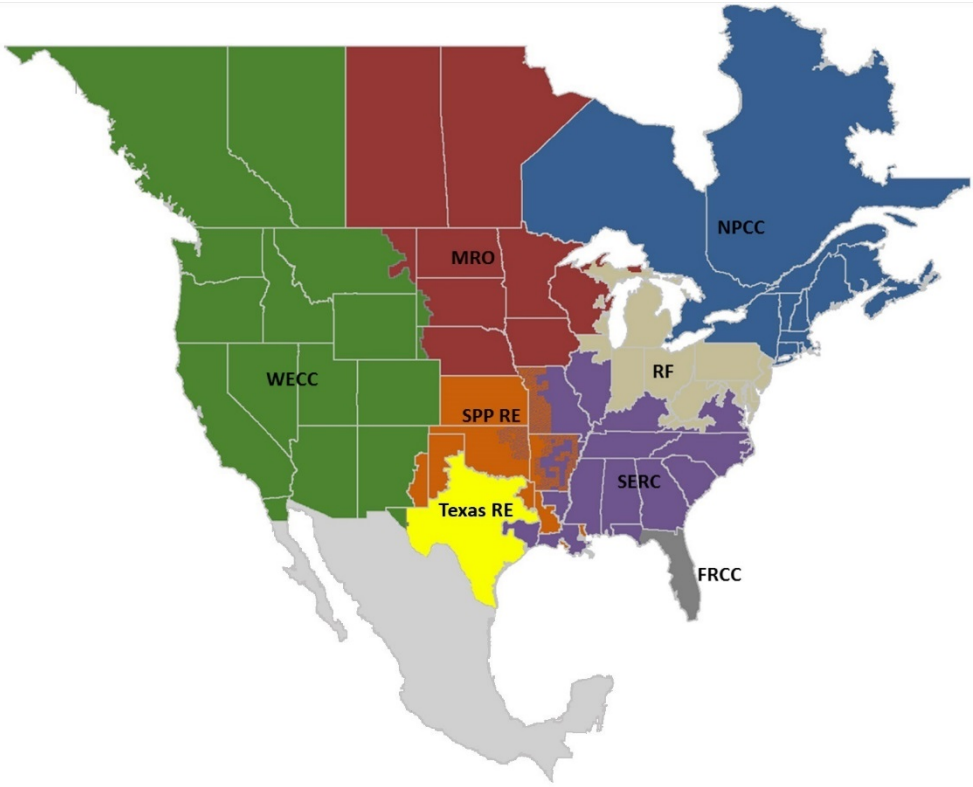
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable 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.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The highlighted areas denote overlap as some load-serving entities participate in one RE while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Disclaimer

The guidance contained in this document represents suggestions on particular topics to be applied by registered entities 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 to their Compliance Enforcement Authority (CEA). This updated User Guide replaces the 2014 Self-Report User Guide, 2014 Mitigation Plan User Guide, and the 2012 Guidance on Self-Reports.

Document Revisions

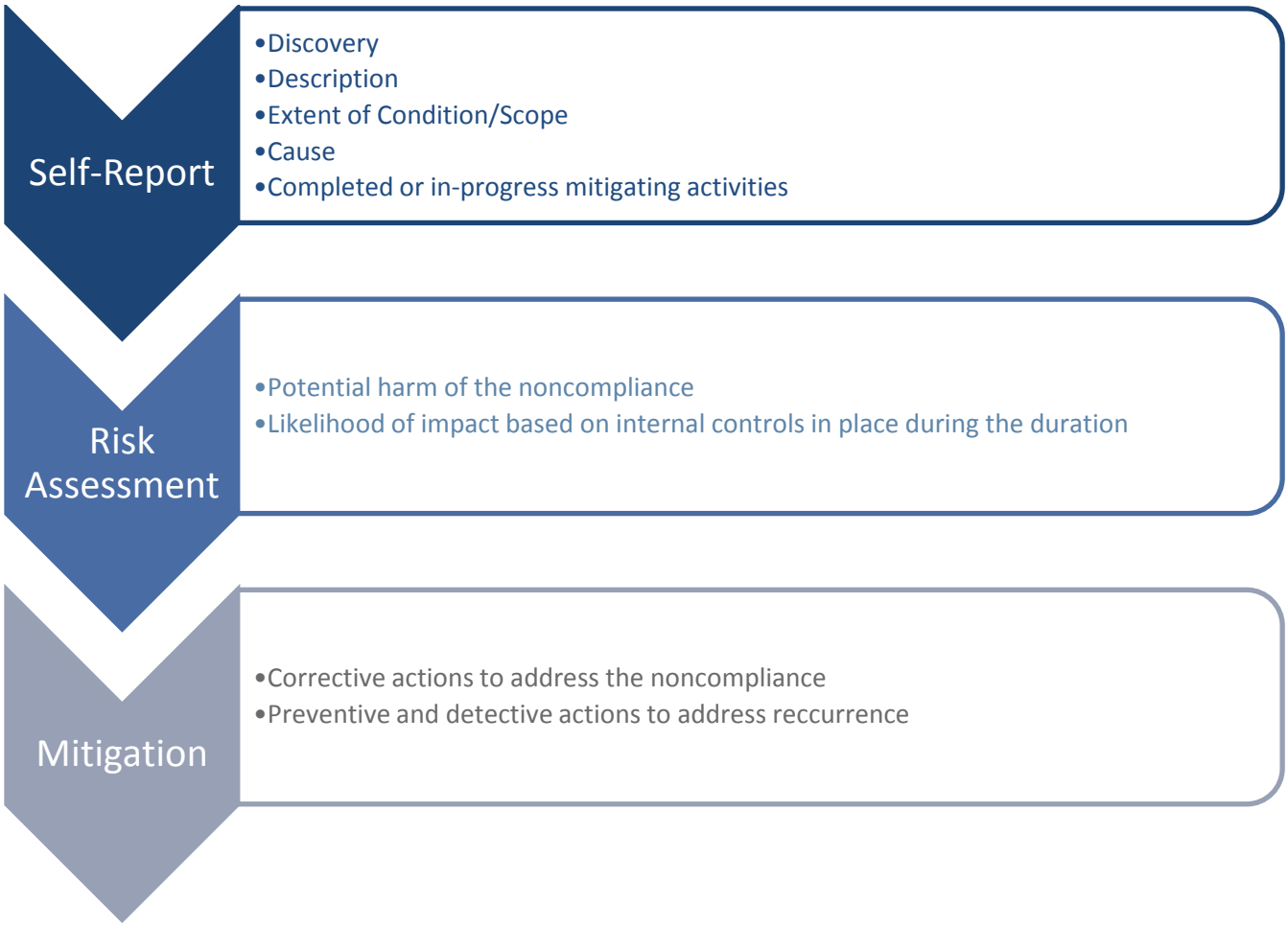
Date	Version Number	Document Changes
January 17, 2014	1.0	
April 17, 2014	2.0	Multiple revisions based on comments received during public comment period, January 22, 2014, through February 21, 2014.
June 12, 2018	3.0	This document is a consolidation of the 2014 Mitigation Plan User Guide, the 2014 Self-Report User Guide, and the 2012 Self-Report Guidance document. Multiple revisions based on comments received from a joint NERC, RE, and industry taskforce, as well as NERC and RE working groups.

Introduction

The ERO Enterprise has 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[1] regarding the circumstances and risk of a noncompliance and the activities an 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, and related mitigation. Accordingly, this User Guide provides guidance to assist registered entities with the submission of Self-Reports and mitigating activities.

This guide supplements information provided in the NERC Compliance Monitoring and Enforcement Program (CMEP), Rules of Procedure, Appendix 4C.[2]

This User Guide is organized as follows:



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

[2] The Rules of Procedure can be found at the following location: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

Chapter 1: Description of the Noncompliance

Prompt and accurate self-reporting is integral to identifying, mitigating, and preventing repeat noncompliance. The NERC Sanction Guidelines direct CEAs to consider whether the registered entity self-reported and whether the registered entity voluntarily undertook corrective action. In evaluating a Self-Report 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 and accurate information in a Self-Report allows 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,[3] and provide more comprehensive information to the CEA as it becomes known. Further, if the registered entity is unsure whether it is in violation of a Reliability Standard, it is best practice to contact the CEA for a preliminary discussion.

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 assess the noncompliance and the risk it poses to the reliability of the BPS. Detailed information within the Self-Report may also result in an earlier decision about disposition. The CEA should also be able to determine if the mitigation and remediation measures described in the Self-Report are adequate to preclude the need for a formal Mitigation Plan. The CEA may consider how long it took the registered entity to self-report the noncompliance once the issue was discovered and whether it was reported in a timely manner. If the registered entity is in the process of identifying all relevant information and scope of the noncompliance, and is concerned the process may take more than three months to complete, the registered entity should contact its CEA to inform it of the noncompliance and ask for guidance on when it should submit the Self-Report.

Multi-Region Registered Entities (MRREs) in the Coordinated Oversight Program should follow the requirements of the program to identify which CEA should receive the Self-Report and mitigating activities.[4] Nevertheless, the guidance contained in this user document would still apply for these entities regardless of the CEA receiving the submittal.

For MRREs, a reporting entity should ensure all facts, risks, and mitigation descriptions refer to the facilities or assets that are affected by the reported noncompliance with the requirement, even if it pertains to a different registration than that assigned to the reporting entity.

Description of the Discovery of the Noncompliance

Within its Self-Report, the registered entity should describe how and when it discovered the noncompliance. The registered entity should also note whether the noncompliance relates to a previous Self-Report or was previously reported to other CEAs.

[3] As discussed below, undue delay in self-reporting may affect how the CEA determines disposition and penalty.
[4] Information on the Coordinated Oversight Program for MRREs is available at: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Coord_Oversight_Guide.pdf

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 was the noncompliance discovered?
    a. Was it discovered by an internal employee or by a third-party?
    b. Was it discovered through self-evaluation, internal review or investigation, or the internal compliance program?
    c. Was it discovered in preparation for, or during a Compliance Monitoring engagement (i.e., Audit, spot check, self-certification, etc.)?
    d. Was it revealed through an event or other operational occurrence?
        i. If it was through an event, please provide the date of that event and, if applicable, the category of the event.[5]
    e. If discovered through detective controls, explain how the detective control led to the discovery of the noncompliance. In addition, the entity should provide an explanation of the detective control's adequacy, or if it needs improvement to help detect similar issues earlier.
    f. What date did the 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 a same or similar noncompliance been previously reported to the same or other CEA(s)?
    a. If so, include date submitted, NCR of the submitting entity, 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.

In order for the CEA to evaluate the nature of a reported noncompliance, a registered entity should include at least the following information in its Self-Report:

1. The Reliability Standard and Requirement(s), as well as all sub-Requirement(s) at issue, and the registered functions at issue. The correct version of the Standard is based on the start date of the noncompliance. For example, if a noncompliance with CIP-007 had a start date of October 1, 2015, and was reported in November 1, 2017, the entity would report the noncompliance as CIP-007-3.[6] A separate Self-Report should be created for each Requirement with the noncompliance information relevant only to that Requirement. If an entity has noncompliance with several related Requirements caused by a single or related set of conduct, it should contact its CEA prior to submittal to discuss how best to provide that information, i.e., through a single Self-Report or through several Self-Reports.
2. 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 scope of the noncompliance, which includes but is not limited to, the number of total affected employees, the type of affected systems (e.g., relays, CTs/PTs, batteries, etc.), and the number of devices and descriptions, intervals, and relevant portions thereof. The registered entity can review the language of the Reliability Standard/Requirement, the measures in the Standard, the Reliability Standard Audit Worksheet, the Violation Severity Level, and the implementation plan, as a guide for what type of information would be beneficial in describing the noncompliance.

[5] *See* Event Analysis Program document available at: https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx
[6] *See* NERC Standards webpage for the effective dates of the Reliability Standards. http://www.nerc.net/standardsreports/standardssummary.aspx

   b. The size, nature, criticality, and location of the facility or assets where the noncompliance occurred.
   c. For CIP-specific noncompliance, include the location of affected assets (within an Electronic Security Perimeter or Physical Security Perimeter, Control Center, etc.) and type of asset (BES Cyber Asset, Protected Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System, etc.).
3. Identify the duration of the noncompliance, including start and end dates, and an explanation for those dates, if known. The start date would be the earliest known occurrence of the noncompliance, the enforceable date of the Standard, the prior mitigation completion date for the same Standard and Requirement, or the end of a previous Compliance Audit with no findings of noncompliance. The end date would be when the noncompliance is corrected (remediated), which is not necessarily the mitigation completion date.
4. The time horizon of the noncompliance, e.g., did the noncompliance impair or threaten real-time operations or day-ahead operations planning?[7]
5. The system conditions at the time of the issue, for example, N-1, misoperations, extreme weather, and any extenuating circumstances.
6. Whether the noncompliance was isolated or a systemic/general control failure potentially impacting multiple processes/systems.

Scope or Extent of the Noncompliance, if Known

Establishing the scope or extent of condition is integral to successful mitigation. If the registered entity does not identify the full scope of the noncompliance, the likelihood for repeat occurrences increases.

If a registered entity determines that performing the extent of condition review would hinder notification to the CEA of the noncompliance in a timely manner, then this step can be included within the mitigating activities. In those circumstances, a registered entity should then perform its extent of condition review and provide information that is more comprehensive to the CEA when submitting the mitigating activities for approval.

In all cases, no matter if a registered entity performs the extent of condition review at the time of discovery or through the mitigation of the noncompliance, the CEA would expect a registered entity to identify the full scope 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 extent of condition review was appropriate. The extent of the scope review may differ based on the facts of the noncompliance. For example, if the noncompliance centers on a Microsoft patch, the scope may be all facilities that include Windows Cyber Assets. If the entity can show noncompliance occurred with a brand of relay only used in one station, there may be no need to consider all other facilities. Therefore, the registered entity needs to provide the details of the scope or extent of condition review and an explanation as to how the registered entity determined the correct scope.

Depending on the nature of the noncompliance, the following could be considered as part of determining the scope of the noncompliance:

1. Other affiliate companies or facilities across its corporate structure.
2. Procedures, assets, facilities, or personnel that are directly affected or could be affected as part of the noncompliance.

[7] Information on specific FERC-approved time horizons can be found within the text of each Reliability Standard. Additionally, there is a general definition document on what a time horizon is for a Reliability Standard.
http://www.nerc.com/pa/Stand/Resources/Documents/Time_Horizons.pdf

3. Other Reliability Standards, to see if any were also violated based on the facts of the reported noncompliance.
4. Prior compliance history involving similar conduct, if known.
5. Whether the scope changed from what was originally reported (e.g., additional devices/facilities/personnel found to be in scope).

The registered entity may include any additional known instances in the Self-Report or, if found later, in the Mitigation Plan or scope expansion. Once the Mitigation Plan or mitigating activities are approved by the CEA, the registered entity should contact its CEA to discuss whether additional instances should be self-reported separately or included as part of a revised Mitigation Plan or mitigating activities.

A registered entity should also review the facts and circumstances of the noncompliance to see if any other Reliability Standards also could pertain. For example:

> If a registered entity failed to test and coordinate the results of its Real Power capability under MOD-025-2 then it could have also have failed to perform the necessary verification under PRC-024-2.
>
> An entity discovered that the configuration data was outdated in its automated system manager and the baseline configuration data was not being uploaded into the automated system manager. As a result, the entity determined that baseline configurations were not monitored for changes every 35 calendar days as required by CIP-010-2 R2 Part 2.1, and therefore baseline configurations were not updated within 30 calendar days of the changes as required by CIP-010-2 R1 Part 1.3.

Causes of the Noncompliance

All noncompliance must have the cause(s) identified prior to final disposition. The listed cause(s)[8] of noncompliance should be consistent between the facts of the noncompliance, the risk(s) it posed, and the actions taken to mitigate and prevent recurrence.

A registered entity should identify and include in its Self-Report all contributing causes of noncompliance in order to effectively correct the instant issue and prevent recurrence. If identifying the contributing causes would prevent the registered entity from notifying the CEA of the noncompliance in a timely manner, then that step can be part of mitigation.

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 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 to take that fact into consideration.

Thorough causal analysis helps solve issues by attempting to identify the cause(s) of events (e.g., weak key controls for contractors) so that 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 likelihood of recurrence can be reduced. A causal analysis should be performed by the registered entity for all noncompliance, regardless of the discovery method (i.e., Self-Report, Audit, Spot Check, Self-Certification, etc.). This analysis should tie directly to

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

the mitigation in either the formal Mitigation Plan or the informal mitigating activities. In this example of weak key control, 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?** And so on.

There are many methods that can be used to determine the cause(s) of noncompliance. The guidance, "Cause Analysis Methods for NERC, Regional Entities, and registered entities," as well as several other references noted in ***Appendix D – Reference Documents,*** are designed to provide a reference of the 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, entities should establish a repeatable cause analysis process that they consistently apply when analyzing noncompliance.

While there is often overlap between different causes and other areas requiring additional controls, and each needs to be explained, the cause(s) explanation needs to be included specifically in the mitigation documentation. Sometimes a "cause and effect" (e.g., A caused B, then B caused C, and then C caused the noncompliance) chain can explain the cause. Caution should be taken 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 underlying multiple causes.

Sometimes noncompliance can be caused by undocumented knowledge, process, or procedures (e.g., 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. In this case, ensure that the processes or procedures become documented and that training on updated and newly documented procedures is provided 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 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 just a symptom of a potentially larger problem?
5. With respect to the cause of the noncompliance, were there extenuating circumstances?

Completed or In-Progress Mitigating Activities

Registered entities' Self-Reports should include a comprehensive description of any mitigating activities and whether they have concluded or are still in progress. The mitigating activities must correct the issue, address the contributing cause(s), and prevent recurrence. If a Mitigation Plan is necessary, the CEA will inform the registered entity. Having comprehensive information on such actions early in the process will help expedite the CEA review of the matter. Additionally, if the registered entity knows the future activities it will take to mitigate and remediate the noncompliance as well as the cause, it should also include those actions in the Self-Report. Providing this information in the Self-Report, will allow the CEA to better analyze whether the registered entity would need to submit a formal Mitigation Plan or if the submittal of mitigating activities in the Self-Report is adequate.

At the Self-Report stage, the CEA has not determined whether it will process the matter through an enforcement action or through either Compliance Exception or Find, Fix, Track, and Report. Therefore, it is in the registered entity's best interest to provide as much detail on the noncompliance and the actions it has taken or will take to mitigate the noncompliance.

Coordinated Oversight

If a registered entity is part of the Coordinated Oversight Program for MRREs, it is expected to report any noncompliance to the Lead Regional Entity (LRE).[9] The LRE will coordinate with the Affected Regional Entity (ARE) so there is no need for duplicate reporting.[10] 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. For Self-Reports related to specific facilities within the ARE footprint, the LRE will notify the ARE and determine the next steps required to designate which CEA will administer the processing of the noncompliance. The LRE will assign a single NERC tracking ID for each of the registered entity's self-reported instances of noncompliance. When conducting the extent of condition review, the entity should discuss with the LRE how to organize the results of the extent of condition review. The MRRE should look at all of the entities and facilities that are part of the MRRE group.

[9] *Supra* n.2. and the *ERO Enterprise Procedure for Coordinated Oversight Program* provided at: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Coord_Oversight_Guide.pdf.

[10] 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 the guidelines to help registered entities assess the risk to the reliability 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 of the BPS as either **minimal, moderate, or serious**.

Risk is the potential impact to reliability multiplied by the likelihood of that impact occurring. In other words, a risk is a potential problem — something to be avoided if possible, or, if unavoidable, the likelihood and/or consequences of which must be reduced. 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 of the BPS considers a variety of inputs, including the particular entity's specific systems, devices, activities, and footprint. The risk also considers any compensating or mitigating factors and internal controls that existed during the period of noncompliance, in addition to any actual impacts caused by the noncompliance.

Risk assessments must be based on facts existing at the time of the noncompliance, and not on assumptions, or facts that develop later. Nevertheless, if an entity identifies relevant information during its extent of condition review or mitigation, it should include that information in its risk assessment. For example, if an entity failed to set its generator voltage protective relays but after reviewing the settings, determined there were no modifications necessary, the entity would still need to address the risk posed by potentially inaccurate trip settings and indicate that no modifications were necessary.

Risk Evaluation

The first step in risk assessment is an evaluation of the potential impact or harm that could have occurred to the facilities, assets, or BPS as a result of the noncompliance. 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, e.g., during an Energy Emergency or when other emergency or special operating procedures were in effect?
2. What are the size, nature, criticality, and location of the facilities at issue?
3. How many assets were at issue and what was the nature and function of the asset(s)?
4. What other systems, facilities, or staff are exposed to the same failure modes?
5. Were there any misoperations, or exceedances of system operating limits or interconnection reliability operating limits during the course of the noncompliance?
6. Was there any potential for loss of a Protection System device, degradation or loss of a BES element, loss of a BES Cyber System or information, or providing unauthorized access to BES Cyber Systems?
7. Was there potential to affect any CIP-005-5 or CIP-007-6 controls that may have impacted CIP Cyber Assets?

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 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 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, e.g., an event on the system, and the risk should indicate whether the noncompliance contributed to the event or if it occurred as a result of the event. The risk should also take into account the size and location of the facilities where the noncompliance took place. For instance, if the issue only affected a single generator in an 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. To the registered entity's knowledge, this would address any negative impact to the facilities, assets, resources, equipment, Cyber Assets, the BPS, etc. The registered entity needs to provide any relevant information (such as extent of condition or scope evaluation) to the CEA so it can complete the risk assessment evaluation.

Risk assessments should be specific to the entity and the BPS and its existing controls mitigating the risk. For example, if an entity with significant generation has failed to update its access lists within seven days (instead updating five days late), but also has multiple layers of protections (PRAs, employees left in good standing, monitoring of access, etc.), then the MW of generation would not itself raise this to a "moderate" risk level.

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 (internal controls, size of facilities, early detection, etc.) in place at the time of the noncompliance. The analysis generally involves identifying the duration or scope of the issue in conjunction with internal controls (preventive, detective, and corrective), or redundancies (backups or other entities performing the same function, for example a failure to perform CT maintenance on redundant CTs when the main CTs were tested and maintained in a timely manner) in place at the time of noncompliance. When the registered entity evaluates the likelihood of the impact occurring, it should also 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 on any internal controls that were in place that quickened the discovery of the noncompliance, shortened the duration of the noncompliance, or reduced the severity of the impact of the noncompliance.

If there were internal controls in place, describe how effective the 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 could be implemented in an automatic or manual manner. Controls will vary from entity to entity because no two 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
5. Internal audit programs

The registered entity must also include steps that will reduce or eliminate risk to the BPS while mitigation is being implemented. 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 those steps it has already taken or which are in place to reduce or eliminate risk to the BPS.

Risk of Possible Additional Instances

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 other instances. As a part of its scope determination, the registered entity identified how widespread the issue was. Here, the entity should identify how widespread the issue could have been, before mitigation began. For example, if the registered entity had a vegetation contact due to program deficiencies, the registered entity would want to provide the risk posed to other lines using that same program and assess when those lines were last checked to see if there could be possible encroachments. Additionally, evaluation of prior compliance history will provide the entity with an understanding of whether its mitigating activities were deficient due to a misidentified cause, 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 violations?
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 be put into place to prevent recurrence?

For more information of what needs to be included in the Mitigation Plan to address risk and recurrence, please see ***Prevention of Future Reliability Risk*** and ***Interim Risk Reduction*** in Chapter 3.

Chapter 3: Mitigation of the Noncompliance

This section describes the type and quality of information related to Mitigation Plans and mitigating activities that a registered entity must submit in order to allow for a prompt evaluation. For most minimal and some moderate risk noncompliance, robust mitigation and remediation descriptions included in a Self-Report may be sufficient and a CEA would not require a formal Mitigation Plan. Therefore, it would be appropriate for a registered entity to include as robust a description as possible in its Self-Report. While the benefits of registered entities submitting more thorough and timely Mitigation Plans 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 of the BPS. This guide supplements information provided in Section 6.0 of Appendix 4C of the NERC Rules of Procedure, by providing further guidance on what should be included in a Mitigation Plan.

Considerations for a Formal Mitigation Plan vs. Informal Mitigating Activities

This section describes the differences between a formal Mitigation Plan and informal mitigating activities. The biggest difference is that the formal Mitigation Plan is a documented plan that has specific timing considerations that apply to it per Section 6.0 of Appendix 4C of the NERC Rules of Procedure. Mitigating activities do not require formal milestones or duplicative descriptions of discovery, contributing cause, or risk—as the registered entity would have provided that information in the Self-Report. Mitigation Plans require formal milestone dates and standalone descriptions of discovery, facts of the noncompliance, contributing cause, and risk—regardless of what the registered entity previously submitted in a Self-Report.

What is a Mitigation Plan and Mitigating Activities?

A *Mitigation Plan* is a formal action plan developed by a registered entity to (1) correct a noncompliance with a Reliability Standard, (2) address the causes of the noncompliance, and (3) prevent recurrence of the noncompliance. A registered entity may cover multiple instances of the same Standard and Requirement in one Mitigation Plan. However, for cases where an issue causes multiple noncompliance of multiple Standards and/or Requirements, a registered entity should create a separate Mitigation Plan for each requirement with the information relevant only to that requirement. The Mitigation Plan is subject to the formal review and acceptance process as described in Section 6.0 of Appendix 4C of the NERC Rules of Procedure.

Mitigating activities are sets of tasks developed by a registered entity to (1) correct a noncompliance with a Reliability Standard, (2) address the cause of the noncompliance, and (3) prevent recurrence of the noncompliance. Registered entities typically submit mitigating activities as part of the reporting process when already completed or when the expected completion date is less than one year.

Using Mitigation Plan vs. Mitigating Activities

Some of the key differences between Mitigation Plans and mitigating activities are identified below:

Requirement	Mitigation Plan	Mitigating Activity
Actions & Tasks	Formal action plan with documented milestones.	List of tasks expected to be completed by a set date.
Milestones	Needs milestones for future activities that are no greater than three months apart. CEA has the authority to check-in and request updates regarding each milestone.	No milestones required, but tasks should ideally be completed within one year. The CEA may inquire on a periodic basis regarding the progress.
Completion	Needs an expected completion date - cannot be before the last milestone date.	Needs an expected completion date and a justification for the time needed to complete the activities.
Duration	Typically used for long-term action plans or plans where regular milestones or check-ins may be necessary.	Typically used for already completed or short-term plans where tasks might already be completed or are expected to be completed within a year.
Documentation	Formal process which is bound by the CMEP requirements for timely submittals, review, and acceptance. Also submitted to FERC as a standalone document.	Informal process where the tasks to be completed are typically included in the disposition document. Review and approval is performed as part of the disposition of the noncompliance. No separate submittal to FERC outside of the final disposition.
Completion	Certification of completion and evidence supporting completion of mitigation by the registered entity is required. The CEA may then choose how to verify depending on the risk and disposition, and will issue a formal verification of completion document.	No formal certification of completion required from the registered entity, but it would still need to notify the CEA of the actual completion date and provide evidence of completion as instructed by its CEA. The CEA may choose to verify, but verification is not required.
Disposition track	Typically used for moderate or serious risk violations that are processed as Spreadsheet NOPs or Full NOPs.	Typically used for minimal and some moderate risk issues that are processed as Compliance Exceptions or FFTs. Nevertheless, a CEA may permit robust and well-described mitigating activities for all risk levels—including noncompliance posing a serious or substantial risk to the reliability of the BPS.

Contents of Mitigation Plan vs. Mitigating Activities

What should be included in a Mitigation Plan?

A Mitigation Plan 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, address the risk posed by the noncompliance and reduce or mitigate that risk, especially during the interim while actions are being implemented. A Mitigation Plan is a standalone document that must contain all the information to understand the noncompliance. Even if an entity has provided a detailed description of the facts, cause, and risk in its Self-Report, if the entity proceeds with or is required to submit a Mitigation Plan, that information should be included in the plan.

Mitigation Plans should address each of the following:

1. Scope/Description of Noncompliance
2. Cause of Noncompliance
3. Additional relevant information regarding the identification of the noncompliance, when necessary
4. Corrective, Preventive, and Detective Actions
5. Milestones
6. Proposed Completion Date
7. Interim Risk Reduction
8. Prevention of future occurrences of similar noncompliance

What should be included in mitigating activities?

Mitigating activities should include: 1) corrective actions to mitigate the noncompliance; 2) preventive controls to reduce the likelihood of a future occurrence; and 3) detective controls to identify potential future noncompliance quickly. The mitigating activities should also address the risk posed by the noncompliance, especially while activities are ongoing.

Although not included in the mitigating activities discussion, the entity should have addressed the description/scope of the noncompliance, the cause, and the risk determination in its Self-Report.

Registered entities are strongly encouraged to take prompt steps to remediate noncompliance as soon as it is discovered.

Mitigating activities should address the following:

1. Cause of Noncompliance
2. Corrective, Preventive, and Detective Actions

Contents	Mitigation Plan	Mitigating Activities
Scope and description of the noncompliance	Required to be included within the Mitigation Plan—even if included in other documents.	Not separately required if included in the discovery document.
Cause of the noncompliance	Required to be included within the Mitigation Plan—even if included in other documents.	Not separately required if included in the discovery document.
Corrective actions	Required to be included within the Mitigation Plan—even if included in other documents.	Required.
Detective, Preventive and Corrective actions	Required to be included within the Mitigation plan—even if included in other documents.	Required.
Milestones	Required (if mitigation extends more than three months into the future).	Not required.
Expected Completion Date	Required.	Required.
Interim Risk Reduction	Required to be included within the Mitigation Plan—even if included in other documents.	Not separately required if included in the discovery document.

Prevention of Future Risk to Reliability	Required to be included within the Mitigation plan—even if included in other documents.	Not separately required if included in the discovery document.

Mitigation of the Noncompliance

This section applies to both Mitigation Plans and mitigating activities and provides a high-level summary of what should be included. The ***Milestones (Mitigation Plans only)*** discussion is only applicable for Mitigation Plans, the other sections apply to both Mitigation Plans and mitigating activities. For detailed requirements of scope, contributing cause, and risk, refer to Chapters 1 and 2 above. Registered entities should take prompt steps to address the noncompliance upon discovery.

Description of the Noncompliance

The registered entity should include the complete description of the noncompliance.

Sections ***Description of the Discovery of Noncompliance*** and ***Description of Noncompliance*** provide detailed information that should be included in the Mitigation Plan or in the Self-Report to capture the relevant facts and circumstances of the noncompliance.

Scope of the Noncompliance

The registered entity should note any changes in the originally reported scope of the noncompliance. When identifying changes in the scope 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 scope determination.

The mitigation should include a narrative describing the comprehensive review by the registered entity to verify the full scope or extent of condition of the noncompliance, which the CEA may review to determine how the extent of condition was performed.

Section ***Scope or extent of the noncompliance, if known*** provides in detail the information that should be included in the Mitigation Plan or in the Self-Report to address the full scope.

Additional Instances Identified During Mitigation

A registered entity is required to submit any additional instances of noncompliance that occur during the period the accepted Mitigation Plan is being implemented. The registered entity should work with the CEA on how it should submit the information, as there will need to be coordination on how to handle these additional instances. Section 6.3 of Appendix 4C of the NERC Rules of Procedure provides that upon completion of the accepted Mitigation Plan, the CEA will notify the registered entity that any findings of noncompliance with the applicable Reliability Standard during the period that the accepted Mitigation Plan was being implemented have been waived and no penalties or sanctions will apply. This section is intended to encourage a registered entity to identify the full scope of a noncompliance in order to mitigate and remediate all instances—thereby preventing future instances. This safe harbor applies once the CEA has an accepted Mitigation Plan or mitigating activities; therefore a best practice would include early submission of robust mitigating activities that include an expansion to identify scope.

Cause of the Noncompliance

The registered entity should also identify all contributing causes of the noncompliance. The purpose of identifying the causes is to learn what caused the problem in order to identity the actions needed to correct the issue and prevent it from occurring again. For effective mitigation, the actions that will reduce the likelihood of noncompliance recurring should be tied to the contributing cause(s).

While there is often overlap between different cause/correction areas, and each needs to be explained, the cause explanation needs to be included specifically in the mitigation documentation. Sometimes a "cause and effect" chain (e.g., A caused B, then B caused C, and then C caused the noncompliance) can illustrate the contributing causes. Caution should be taken when relying on a cause and effect chain to avoid an overly narrow focus. A broader view of the issues may often result in registered entity mitigation efforts that more thoroughly address underlying causes.

Section ***Causes of Noncompliance*** details the information that should be included in the Mitigation Plan, or in the Self-Report and updated in the description discussion of the final disposition document for mitigating activities.

To ensure the entity properly addresses the cause, the registered entity should review its own compliance history to see if a same or similar issue 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.

Corrective Actions - Current Issue

Corrective actions should be designed with the primary intent to remediate the noncompliance and restore compliance with the Reliability Standard(s) as quickly as possible. Corrective actions should also consider the cause and any other Reliability Standards impacted by the noncompliance. After determining the corrective actions, 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. The registered entity should document any training, including training materials, attendee list, etc.

Any actions that are completed prior to submittal of the Mitigation Plan or mitigating activities, or that are in-progress as part of the initial reporting to the CEA, should also be included in this section.

Section ***Completed or In-Progress Mitigating Activities*** details the information that should be included in the Mitigation Plan, or in the Self-Report and updated in the final disposition document for mitigating activities to report any actions completed.

Preventive and Detective Actions - Prevention of Recurrence

Preventive and detective actions should be taken with the primary intent to detect the noncompliance in advance and to prevent it or to reduce the likelihood of recurrence. 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.

Milestones (Mitigation Plans only)

Milestones are required for Mitigation Plans when a proposed completion date is more than three months from submission. Milestones should be no more than three months apart and are used to track the registered entity's progress.[11] Milestones should be relevant, measurable, and realistic for meeting the proposed completion date.

[11] Milestones that are complete at the time of submission may be more than three months apart.

Although milestones are not required for Mitigation Plans that are completed in less than three months, registered entities are encouraged to have milestones to help both the CEA and the registered entity track progress and identify any potential issues that could impact the proposed completion date.

Proposed Completion Date

The proposed completion date is the expected date when all actions in the Mitigation Plan or mitigating activities, including any milestones, will be completed. The registered entity should consider the scope of actions outlined in the mitigation as well as the assumptions, risks, and dependencies that may impact the proposed completion date.

There are times when a proposed completion date may need to be extended after a Mitigation Plan has been accepted. Section 6.3 of Section 4C of the NERC Rules of Procedure states that at the CEA's discretion, the completion deadline may be extended 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.

For formal Mitigation Plans, a request for an extension of any milestone or the completion date of the accepted Mitigation Plan by a registered entity must be received by the CEA at least five (5) business days before the original milestone or mitigation plan completion date. For mitigating activities, the entity needs to inform the CEA, preferably in writing, of the new date and the reason for extension, pending acceptance by the CEA.

Interim Risk Reduction

The registered entity must include steps that will reduce or eliminate risk to the BPS while mitigation is being implemented. The risk reduction steps must be specific for the risks identified. This step is especially critical for plans with longer durations. In determining interim actions and activities, registered entities should identify and address any risks to the BPS that may exist while the mitigation is in progress. It should include those steps that may have already been taken 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.

For more information on assessing risk, refer to ***Chapter 2: Risk Assessment.***

Prevention of Future Risk

Prevention of future risk to the reliability of the BPS should detail how the successful completion of the mitigation minimizes the probability that the registered entity will violate the same or similar Reliability Standards again. Additionally, the registered entity should state how the mitigating actions taken will prevent future risk to the reliability of the BPS.

For more information on assessing risk, refer to ***Chapter 2: Risk Assessment.***

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 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. This was because other surrounding undergrowth vegetation was over 10 feet tall, making it difficult to determine the distance between the line and the vegetation aerially.
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 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.

Reliability Standard - FAC-003-4 R2	Lacking	Acceptable
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.

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.
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. Finally, a backup process was implemented 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 add seven Physical Access Control System (PACS) panels to its baseline configuration within 30 days, as required under CIP-010-2 R1, part 1.3.	While conducting an internal review, the entity discovered a discrepancy between the baseline configuration and the devices' running configuration. During the investigation into this issue, the entity determined that when it deployed the configuration to the network devices, it did not document all of the ports on the baseline configuration. Specifically, the entity discovered that it had failed to add seven newly installed PACS panels to its baseline configurations within 30 days, as required under CIP-010-2 R1, part 1.3. Starting in 2017, the entity began installing new PACS for its primary and backup Control Centers. As part of this process, personnel began to install a number of PACS access control panels at various Control Center locations. During this process, personnel selected an incorrect workflow for seven of the PACS that was not intended for new NERC Cyber Assets. After identifying the issue, the entity performed an additional review to focus on potential workflow issues.
Cause	The cause was an inadequate process around baseline configurations.	The cause was an insufficient change management process. Specifically, the entity lacked a documented process to ensure its personnel properly identified all new NERC Cyber Assets, and did not provide an explicit location option for PACS panels in the workflow.
Risk Assessment	The risk was reduced because the BES Cyber Systems 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 PACS network, restricting any unauthorized access by the panels to the BES Cyber Systems.	The entity's insufficient understanding of the change management process and of a documented process for properly identifying NERC Cyber Assets could lead to unknown vulnerabilities that could negatively affect the BCSs, including the deletion/manipulation of undocumented applications that are determined to be necessary for Cyber Asset use. The risk was reduced because the entity had multiple controls in place to prevent the likelihood of the potential impact. First, the panels at issue were locked and tamper-protected, and only two entity staff members had access to the panels. Second, the seven panels at issue were all configured in an encrypted mode, which helps ensure the integrity of the data and prevent the introduction of malicious code. Third, the BES Cyber Systems for the entity are located inside an ESP and are protected by firewall(s), which control access to the ESP systems, as well as additional layers of firewalls specific to the PACS network restricting any unauthorized access by the panels to the BES Cyber Systems. Fourth, in the event of a breach of the seven panels, the devices would not accept invalid data formats. In the event the data was sent in an unrecognizable format, the panels would initiate a reboot, which would send an alert to the entity's security operations console. No alerts

Reliability Standard - CIP-010-2 R1	Lacking	Acceptable
		were sent during the time period at issue. Fifth, if the panels were to fail, the biometric readers at the door would fail to close and use the access credentials stored locally. Sixth, all access points to the Physical Security Perimeters (PSPs) are monitored by cameras and the entity security personnel at all times. Finally, the entity possessed a number of cyber security systems, including automated security event monitoring controls, 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 panels 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.
Mitigation	To mitigate this issue, the entity: 1) conducted a review of all network devices to determine if there were any other discrepancies between the baseline configuration and the running configuration; and 2) completed the baseline configuration for the PACS panels.	To mitigate this issue, the entity: 1) completed the baseline configuration for the seven panels; 2) modified the tool to provide an explicit option for PACS panel location within the designated new build workflow; 3) shared responses to a lessons learned questionnaire that identified problems regarding this issue during the project delivery portion of the PACS installation project; 4) 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; 5) revised the process document for building new Cyber Assets; 6) revised the technical architecture documents to include a decision tree for the project to evaluate Cyber Assets and determine applicability to NERC CIP Standards; 7) modified the documented processes for new Cyber Assets, to include explicit guidelines for identifying all NERC Cyber Assets during the new build process; 8) revised the applicable new build workflow processes in the tool to preclude closing new build requests until all applicable baseline activities are performed; 9) 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 10) 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 19 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-007-5 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

This checklist is intended 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 through self-evaluation, internal review or investigation, or the internal compliance program? If discovered through detective controls, explain how the detective control led to the discovery of the noncompliance. Was it discovered in preparation for, or during, a Compliance Monitoring engagement (i.e., Audit, Spot-Check, Self-Certification, etc.)? Was it revealed through an event or other operational occurrence?
  - ✓ When was it discovered?
  - ✓ What period elapsed between identifying and reporting the noncompliance to the CEA? If there is a gap exceeding three months between identifying the noncompliance and reporting the noncompliance to the CEA, is there an explanation?
  - ✓ Has the same or similar noncompliance been previously reported or reported to other CEAs?
- Does the Self-Report describe the noncompliance?
  - ✓ Is the noncompliance adequately described by tying the description to the Reliability Standard/Requirement?
  - ✓ Does the description include how the noncompliance occurred?
  - ✓ Has an extent of condition review been performed, and if so, what other procedures, assets, facilities, or personnel were impacted or could be impacted by the noncompliance?
- Does the Self-Report describe the cause of the noncompliance?
  - ✓ Has the cause been completely identified?
  - ✓ Were there any other contributing causes?
  - ✓ Did the entity review its detective processes to determine if anything needs to be added or improved?
- Does the Self-Report include duration information?
  - ✓ What date did the noncompliance begin? What date did the noncompliance end?
- Does the Self-Report address the risk associated with the noncompliance?
  - ✓ What were the system conditions at the time of the issue? For example, did the noncompliance take place while the system was stressed, e.g., during an Energy Emergency or when other emergency or special operating procedures were in effect?
  - ✓ What are the size, nature, criticality, and location of the facilities or assets at issue?
  - ✓ What harm did occur, or what harm could reasonably have occurred?
  - ✓ Were there any misoperations, or exceedances of system operating limits or interconnection reliability operating limits during the course of the noncompliance?
  - ✓ Was there any loss of a Protection System device, degradation or loss of a BES element, loss of BES Cyber System information, or unauthorized provision of access to BES Cyber Systems?
  - ✓ Was there potential to affect any CIP-005-5 or CIP-007-6 controls that may have impacted BES Cyber Assets?
- Does the Self-Report include mitigating activities that include all corrective, detective, and prevention of recurrence actions—if known?
  - ✓ Do the actions relate to requirements in scope?
  - ✓ Do the actions address the cause of the noncompliance?
  - ✓ Does the report include how and when the noncompliance will be mitigated?
  - ✓ Has prevention of recurrence been addressed?
  - ✓ Have all actions taken to resolve the noncompliance and prevent recurrence been included?
  - ✓ Have completion dates for all actions completed prior to submission of the Self-Report been included?

Appendix C: Mitigation Plan Checklist

This checklist is intended to provide a quick outline of the topics discussed in ***Chapter 3: Mitigation of Noncompliance***.

- Describe the scope of the noncompliance being mitigated.
  - ✓ Is the noncompliance adequately described by tying the description to the Reliability Standard?
  - ✓ Does the description include how the noncompliance occurred?
  - ✓ How was the noncompliance discovered? Did the registered entity discover the noncompliance using detective processes?
  - ✓ Has the scope 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?
- Describe the cause of the noncompliance.
  - ✓ Has the cause been completely identified?
  - ✓ Were there any other contributing causes?
  - ✓ If the noncompliance was not discovered by the registered entity, did the entity review its detective processes to determine if anything needs to be improved or implemented?
- Include all corrective, detective, and prevention of recurrence actions.
  - ✓ Do the actions relate to requirements in scope?
  - ✓ Do the actions address the cause 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 prevent recurrence been included?
  - ✓ Have completion dates for all actions completed prior to submission of the plan been included?
- Include milestones as needed.
  - ✓ Have milestones been defined where appropriate (for future actions)?
    - o If milestones are included, do the milestones have sufficient detail?
    - o Are the milestone intervals reasonable?
    - o Are the milestone intervals no longer than three months apart?
  - ✓ Remember to retain evidence to provide proof of completion for all actions taken.
- Include a proposed completion date.
  - ✓ Will all milestones be completed prior to the proposed plan completion date?
- Describe the interim risk associated with the reliability of the BPS while the Mitigation Plan is being implemented.
  - ✓ Does the Mitigation Plan contain interim steps to address this risk?
- Describe the prevention of future risk to the reliability of the BPS.
  - ✓ How will the successful completion of this Mitigation Plan prevent or minimize the probability that your organization incurs further risk of noncompliance with the same or similar Reliability Standards requirements in the future?
- Describe how the Mitigation Plan actions will reduce the likelihood of recurrence.
  - ✓ If the registered entity had prior instances of noncompliance, does it explain how that noncompliance impacts the current issue and how the actions taken in this plan would help to prevent recurrence?

Appendix D: Reference Documents

FERC Guidance or Reference Documents

- *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) http://www.ferc.gov/whats-new/comm-meet/2012/031512/E-3.pdf
- *North American Electric Reliability Corporation*, 134 FERC ¶ 61,209 (2011) (Turlock Order) http://www.ferc.gov/whats-new/comm-meet/2011/031711/E-3.pdf
- *Enforcement of Statutes, Orders, Rules, and Regulations*, 132 FERC ¶ 61,216 (2010) (Revised Policy Statement on Penalty Guidelines) http://www.ferc.gov/whats-new/comm-meet/2010/091610/M-1.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) http://www.ferc.gov/eventcalendar/Files/20080703131349-AD08-10-000.pdf
- *Policy Statement on Compliance*, 125 FERC ¶ 61,058 (2008) http://www.ferc.gov/whats-new/comm-meet/2008/101608/M-3.pdf
- *Revised Policy Statement on Enforcement*, 123 FERC ¶ 61,156 (2008) http://www.ferc.gov/whats-new/comm-meet/2008/051508/M-1.pdf
- FERC Overall Approach to Root Cause Analysis http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/consult-rpt/sec-5-overall.pdf

- 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 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
- 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