NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Self-Logging Program User Guide

November 27, 2018

RELIABILITY | ACCOUNTABILITY



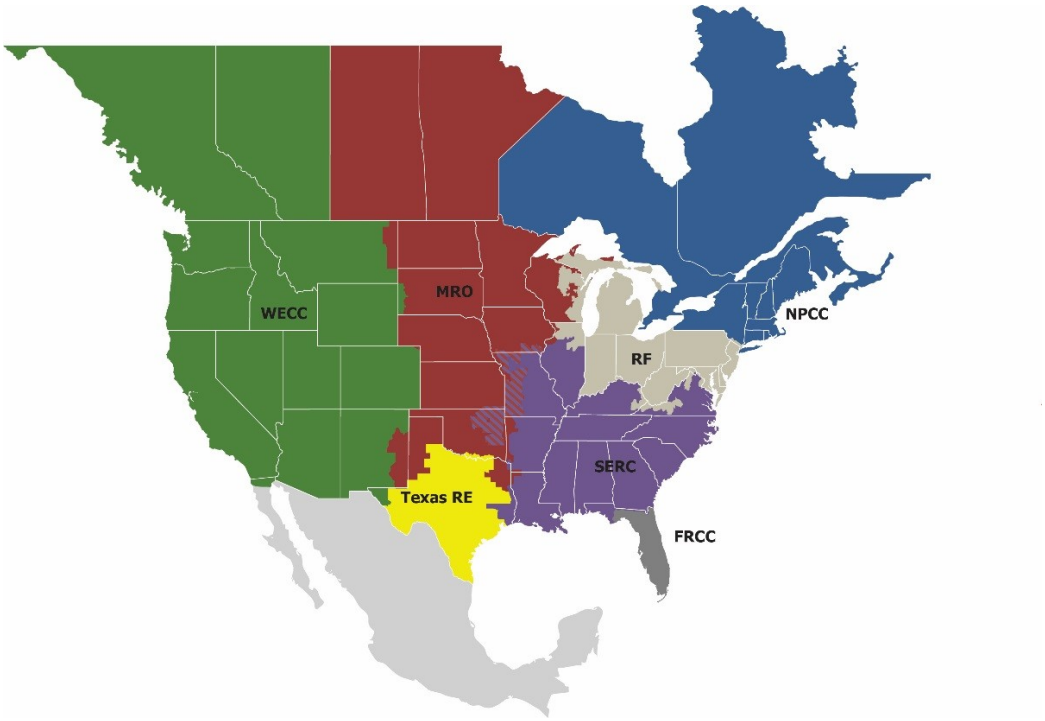

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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 seven 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 seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region 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
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Disclaimer

The guidance contained in this document 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 self-logging instances of noncompliance to an RE.

Introduction

The ERO Enterprise has developed this Self-Logging Program User Guide for registered entities currently admitted to the program, registered entities interested in requesting consideration for inclusion in the program, and other stakeholders interested in the program's administration. This guide provides information to assist registered entities in providing adequate information to aid the REs' determinations of eligibility and in determining the appropriate level of information to include in self-logs. This guide also provides examples of self-logged noncompliance and includes an appendix of additional resources to aid registered entities in obtaining more information. This user guide supplements information provided in the NERC Compliance Monitoring and Enforcement Program (CMEP), Rules of Procedure (ROP), Appendix 4C,[1] Self-Report and Mitigation User Guide,[2] and other guidance and reference documents referenced in Appendix E. This guide is one tool to assist the ERO Enterprise and industry in instituting best practices. It adds clarity to what information is needed to resolve minimal risk issues so registered entities can provide complete facts to REs in self-logs, facilitate expedited processing and review by NERC and FERC, and continue to build regulator confidence in the industry's ability to identify, assess, and correct minimal risk noncompliance.

The Self-Logging Program, which was finalized in May of 2015, provides that if a Compliance Enforcement Authority (CEA)[3] finds a registered entity to be eligible for the program after some level of formal review of a registered entity's internal controls, the registered entity may log noncompliance for subsequent review by the ERO Enterprise in lieu of submitting Self-Reports. The log is currently limited to noncompliance posing a minimal risk to the reliability of the BPS. Under the Self-Logging Program, approved registered entities maintain a log with a detailed description of the noncompliance, the risk assessment, and the mitigating activities completed or to be completed. There is a rebuttable presumption that minimal risk noncompliance logged in this manner will be resolved as Compliance Exceptions (CEs). The RE periodically reviews the logs to affirm CE disposition, and provides the self-log CEs to NERC for posting, at which time they are subject to a 60-day review by NERC and FERC.

Since the inception of the program, the ERO Enterprise has processed approximately 250 self-logged instances of noncompliance. Registered entities have accurately assessed the risk of the noncompliance in the self-logged items that have been posted as CEs. In a small number of instances, the RE determined the self-logged noncompliance posed more than a minimal risk and therefore was not appropriate for CE treatment. Additionally, registered entities are successfully mitigating the noncompliance, as the ERO Enterprise has not been able to identify a subsequent moderate or serious risk issue violation that was caused by the failure to mitigate a self-logged noncompliance.

In 2016, NERC staff performed a review of the Self-Logging Program. This review evaluated the consistency of the REs' practices related to the program and identified any areas for improvement. NERC staff's review confirmed that the REs, in general, are implementing successfully and consistently the Self-Logging Program. NERC staff found that the ERO Enterprise has a more thorough understanding of the risk posed by noncompliance across the BPS because of active participants in the program.

After the process review, the ERO Enterprise designed and issued a survey to two sets of registered entities. The first survey went to registered entities already admitted to the Self-Logging Program. The second went to registered entities identified as potentially eligible. These surveys requested feedback and ideas for additional enhancements to the Self-Logging Program and other areas of improvement to encourage additional registered entity participation

[1] The Rules of Procedure can be found here: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

[2] The Self-Report and Mitigation Plan User Guide can be found here: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Registered%20Entity%20Self-Report%20and%20Mitigation%20Plan.pdf.

[3] "Compliance Enforcement Authority" means NERC or the REs in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards. As there are no entities self-logging under NERC's role of directly monitoring or enforcing compliance, the term "CEA" and "RE" are used interchangeably within this document.

and to continue to leverage the success of the program in the future. This user guide is one of the enhancements identified by registered entity survey responses as an improvement to the Self-Logging Program.

Chapter 1: Benefits of the Self-Logging Program

The Self-Logging Program is continuing to evolve. The ERO Enterprise continues to work with industry to identify potential areas for enhancement to ensure the greatest benefits for the reliability of the BPS. While the future holds the possibility for even more streamlined oversight of minimal risk issues, the ERO Enterprise and participants in the program are already realizing benefits today.

Under the program, REs review the registered entity's submitted log of noncompliance for concurrence with the registered entity's assessment of risk and to determine whether the mitigating activities as provided would resolve the identified noncompliance and prevent recurrence. If the RE concurs, the RE creates the CE and then efficiently concludes the noncompliance in a much shorter time frame as compared to traditional Self-Reports. Registered entities that are accepted into the program receive experience with providing the following:

- A complete description in a concise manner,
- Assessing the risk of noncompliance,
- The type of minimal risk noncompliance to include on self-logs,
- How to log multiple instances of noncompliance with the same Standard and Requirement,
- What information is needed, and
- Identifying the cause and describing the mitigating activities that addressed the noncompliance and the cause.

The ERO Enterprise and industry perform well in these areas. In the most recent annual NERC and FERC review of the CE program, FERC agreed with the risk determinations for 124 of the 126 sampled self-logged CEs.[4]

To realize the benefits of this program, registered entities need to seek entry into the program. RE outreach to registered entities about the requirements, process, and benefits of the program to encourage participation is paramount. Many REs are conducting successful outreach to their registered entities on the benefits of self-logging. The ERO Enterprise's objective is to have high-performing registered entities meet the criteria for entry into the program. NERC and the REs aim to have sufficient information available to any registered entity interested in the program and the resources to assist registered entities in improving their own internal controls to be eligible to self-log.

The Self-Logging Program Demonstrates Registered Entity Responsibility

While there are currently many benefits from participation in the Self-Logging Program, many more may be possible with additional regulator confidence. The ERO Enterprise's efforts to right-size regulation, including implementation of the risk-based approach to determine an appropriate body of Reliability Standards, such as the FERC-supported Paragraph 81 project[5] and the Standards Efficiency Review project,[6] are dependent upon registered entity participation. Registered entities' ability to identify noncompliance, assess risk to the reliability of the BPS, and correct and prevent recurrence of noncompliance posing a minimal risk to reliability gives regulators confidence that industry is monitoring and addressing such risks to reliability. The self-logging program empowers registered entities to monitor their own compliance while focusing on serious risks. Registered entities awarded self-logging privileges have successfully demonstrated the ability to identify, correct, and assess risk in a timely manner due to their robust

[4] "FERC staff also noted a significant improvement in the clear identification of factors affecting the risk before mitigation (such as potential and actual risk), and actual harm, which was identified in all samples. In addition, FERC staff noted that the FFTs and CEs sampled did not contain any material misrepresentations by the registered entities." North American Electric Reliability Corporation, Notice of Staff Review of Compliance Programs, FERC 83 FR 37494 (August 1, 2018).

[5] http://www.nerc.com/pa/Stand/Pages/Project2013-02_Paragraph_81.aspx

[6] http://www.nerc.com/pa/Stand/Pages/Standards-Efficiency-Review.aspx

internal controls and processes, thus supporting an even more streamlined approach to those registered entities' minimal risk issues.

The Self-Logging Program Provides for Efficient Reporting of Noncompliance

Tracking noncompliance on a log as they occur and quarterly batch reviewing by the RE provide some reporting relief to the registered entity as it does not need to develop a Self-Report for each instance of noncompliance. In addition, the self-logging template provides consistency in descriptions across the ERO Enterprise. As registered entities and the ERO Enterprise gain experience with what information the self-logging entity is providing on the spreadsheet, registered entities continue to improve completing the log with all necessary information.

The Self-Logging Program Provides for Presumed Expedited Disposition

Self-logged noncompliance has presumed CE treatment. A CE is an instance of noncompliance that poses a minimal risk to the reliability of the BPS, does not warrant a financial penalty, is mitigated within a year of posting, and is recorded without triggering an enforcement action.[7] From a registered entity's perspective, one of the most significant benefits of CE treatment may be that the noncompliance is not aggravating for penalty purposes or included in a registered entity's compliance history.[8]

The CE is a fast-track disposition method that provides shorter processing times leading to higher efficiency when processing minimal risk noncompliance by reducing certain formal administrative processes associated with individual Self-Reports.[9] The ERO Enterprise processes self-logged noncompliance in nearly one-third the time of CEs discovered through other means, even when taking the time between quarterly log submissions into consideration. NERC attributes this efficiency to the self-logging registered entities' internal controls that help with the identification, analysis, and remediation of the issue correctly and swiftly.

Additionally, because self-logged instances of noncompliance have the presumption of CE treatment, these logs often increase a registered entity's initiative in performing reviews of its own programs proactively, providing visibility on potential areas of weakness and the opportunity to refine or create internal controls to address those weaknesses. Given these advantages, registered entities have shown a greater inclination to identify potential noncompliance through self-logging.[10] Further, NERC has observed that the most common Reliability Standards associated with self-logged noncompliance are the same ones as those associated with other discovery methods. This observation reinforces regulator perception that the registered entities are using the program efficiently to record the most common areas of noncompliance.

The Self-Logging Program Provides Greater Visibility and Knowledge

In addition to efficiency gains, the log is also an ideal tool for the registered entity to conduct trend spotting within its own organization because all minimal risk noncompliance, as well as any associated mitigation, are contained on the log. Additionally, log review and discussion may trigger productive dialogue between the RE and the registered

[7] The CE process is set forth in Section 3.A of the NERC CMEP, Appendix 4C to the NERC Rules of Procedure.

[8] A CE is part of a registered entity's compliance history only when "a later violation classified as 'serious' or 'substantial' follows or occurs because of the registered entity's unsuccessful or partial remediation of the compliance exception(s)." *North American Electric Reliability Corp.*, 150 FERC ¶ 61,108 at 44 (2015) (*February 19 Order*). Furthermore, prior CEs are considered when "assessing any subsequent noncompliance of the same or closely-related Standards and Requirements to determine whether the registered entity should continue to qualify for [CE] treatment regarding the subject of the repeat noncompliance," but "[such] subsequent noncompliance…in and of itself should not disqualify an entity from RAI." *Id.* at 45.

[9] Annual Report of the North American Electric Reliability Corp. on the 2015 ERO Enterprise Compliance Monitoring and Enforcement Program, at 39, *North American Electric Reliability Corp.*, Docket No. RR15-2-000 (Feb. 18, 2016) (2015 CMEP Annual Report).

[10] *See* Comments of MISO at 5, *North American Electric Reliability Corp.*, Docket No. RR15-2-000 (Dec. 3, 2014) ("By encouraging the reporting of the full panoply of a registered entity's compliance issues, the self-logging program facilitates full and open dialogue between a registered entity and its regulators, and gives NERC and the REs a more comprehensive view of the compliance issues facing a registered entity.").

entity regarding risk for the registered entity and potential expansion of mitigating activities to prevent broader issues in the future. This also provides an opportunity for discussion on, among other things, standards involving high-frequency conduct, where a registered entity may show its RE how it is being resilient through its internal controls and mitigating risk when there is a noncompliance.

As the registered entity completes its own risk assessment to determine whether the noncompliance qualifies for self-logging, and because the rationale contained within the log must support the risk assessment, there is an opportunity for the registered entity to conduct more analysis and potentially develop or refine internal controls to prevent or mitigate future occurrences. This additional insight and facilitation of trend spotting benefits the reliability of the BPS by providing an RE a more specific view of risk in its own footprint.

Finally, several registered entities in the Self-Logging Program indicated to NERC that the Self-Logging Program's periodic nature helps support compliance activities and culture by providing timely feedback from the RE regarding minimal risk noncompliance and its mitigation. Those entities believe self-logging is a valuable tool to assist in recognizing and implementing management practices around Reliability Standards.

The Self-Logging Program's Influence on Compliance Oversight Plans

The Self-Logging Program relies on and promotes a closer understanding by REs of registered entities' management practices. It creates motivation and incentives for registered entities to develop and enhance effective controls to identify, detect, and correct instances of noncompliance as they arise.[11] Because the program promotes sharing of information about such controls with the REs, it provides the opportunity to increase regulator confidence and provide input into the registered entity's Compliance Oversight Plan (COP).[12]

[11] Informational Filing of the North American Electric Reliability Corp. on Implementation of the Reliability Assurance Initiative, *North American Electric Reliability Corp.*, Docket No. RR15-2-000 (Nov. 3, 2015).

[12] *See* the ERO Enterprise Guide for Compliance Monitoring sec. 3 (Oct. 2016), for a description of COPs. *See also* the 2018 ERO Enterprise CMEP Implementation Plan – Version 2.1 at 7 (May 2018).

Chapter 2: Eligibility Review

Each RE includes information on its website indicating how a registered entity can request participation through evaluation of eligibility for the Self-Logging Program. This information includes, at a minimum, a centralized email address, or other contact information for the responsible individual or department at the RE. Most REs also have a link to NERC's ERO Enterprise risk-based CMEP page and Self-Logging Program document for more information on the program. Appendix D includes a complete list of and links to the REs' Self-Logging Program resources.

Methodology to Evaluate Eligibility

The RE will determine a registered entity's eligibility for self-logging through an evaluation of the registered entity's controls associated with its ability to identify, assess, and correct noncompliance.[13] To satisfy the evaluation and become eligible for self-logging, a registered entity must demonstrate that it has sufficiently institutionalized processes in place to identify, categorize, prioritize, and mitigate operational risks to reliability. It also must have sufficient internal processes to perform cause analysis to ensure successful corrective and preventive actions.

While each RE's process to review a registered entity's internal controls is slightly different, tailored to match the needs of that RE and entity, NERC's oversight activities have found that all of the RE evaluations are consistent with the requirements of the Self-Logging Program. All REs assess program applicants by examining internal controls, internal compliance programs, and compliance history, including past cooperation and self-assessments.

The best practice for registered entities requesting eligibility is to provide the information on the subjects identified in the three methodology sections of the ERO Enterprise Self-Logging Program document.[14] The nature and extent of the RE's review may vary according to the inherent risk of the registered entity, information on the entity's processes, and the RE's knowledge of the internal compliance program obtained through prior compliance monitoring and enforcement activities. The RE, as much as possible, will use information already in its possession to evaluate a registered entity's eligibility for self-logging. Registered entities are encouraged to engage with the RE throughout the eligibility process. The RE may request additional documentation or a detailed narrative showing the following:[15]

- Evidence the entity has effective processes in place for identifying possible noncompliance with Reliability Standards. Evidence should include the following:
  - How the registered entity identifies and reports possible noncompliance with Reliability Standards;
  - How the registered entity performs an extent of condition review surrounding an identified possible noncompliance; and
  - How the registered entity determines there is no noncompliance (e.g., follow-up, if any, for near-misses).
- Evidence it has effective processes in place to thoroughly investigate the facts, accurately assess the risk, and respond appropriately to the risk surrounding an identified possible noncompliance. Evidence should include the following:
  - How the registered entity assesses risk to reliability posed by possible noncompliance;
  - How the registered entity communicates reliability risk of possible noncompliance to individuals, departments, affiliates, or others potentially affected by the possible noncompliance; and
  - How the registered entity uses the assessment of risk to reliability to respond to the noncompliance.

[13] The ERO Enterprise Self-Logging Program document contains a full discussion of the methodology an RE will use to determine a registered entity's eligibility to self-log.
[14] *Id.*
[15] *Id*.

- Evidence it has identified the cause(s)/root cause(s) of past noncompliance. Evidence may include the following:
  - Processes for identifying and communicating root cause(s) of possible noncompliance, and
  - Processes for trend-spotting possible noncompliance with similar causes.
- Evidence it provides timely and thorough communications to both the employees responsible for mitigation and to relevant RE(s);
- Evidence of an appropriate level of involvement of senior management in the evaluation and correction of noncompliance;
- Evidence of the creation and maintenance of feedback to affected departments to review and correct deficiencies in processes and procedures that have led to noncompliance;
- Evidence that it has effective processes in place for addressing/mitigating identified causes of noncompliance (both cause of discrete noncompliance and prevention of recurrence); and
- Evidence that the entity assesses the effectiveness of past mitigating activities.

The RE will assess whether these internal processes have been properly designed and implemented. The registered entity should provide sufficient, appropriate evidence to support its assertions about the effectiveness of those processes.

Appendix A includes a checklist of examples of possible evidence a registered entity may use to provide a complete picture of its abilities to its RE for entry to the program.

Communications Regarding Determination of Eligibility

The ERO Enterprise has committed to performing reviews for eligibility within a 90-day period. If an RE is unable to complete its review within a 90-day period, the RE would remain in communication with the registered entity and NERC and inform them of any unforeseen circumstances. The ERO Enterprise notes that eligibility determinations of multi-region registered entities (MRREs), regardless of participation in the Coordinated Oversight Program, may require additional time to work with other REs in determining a registered entity's eligibility. REs notify NERC on a monthly basis of new activity in the Self-Logging Program.

Possible Revocation of Self-Logging Privileges

If the RE concludes that any of the registered entity's logged instances of noncompliance are insufficient due to unclear or missing information, unsupported risk determinations, or inadequate mitigation (e.g., recurring instances of noncompliance stemming from the same or substantially similar root cause), the RE may, at its discretion, and as further discussed below:

- Work with the registered entity to correct the unsatisfactory log entries, including, if necessary, asking for additional information or mitigating activities;
- Process the instance of noncompliance through an alternate disposition method; or
- Modify or revoke self-logging privileges, depending on the facts and circumstances of the insufficient log(s).

Specifically, where there is evidence the registered entity failed to make a good faith effort to accurately record or effectively mitigate a logged instance of noncompliance, the RE may revoke self-logging privileges and process the logged instance(s) of noncompliance through a formal enforcement action. For example, if the registered entity knew or should have known that it mischaracterized a logged instance of noncompliance as posing a lesser risk to qualify it for Self-Logging, or if the registered entity knew or should have known that it implemented clearly inadequate mitigating activities that could not reasonably be expected to correct or prevent recurrence of the logged instance of

noncompliance. If the RE revokes or modifies the registered entity's self-logging eligibility, the RE will inform the registered entity and NERC of the basis for that decision.

Chapter 3: Completeness and Accuracy of Logs

Registered entities within the program maintain a self-logging spreadsheet for eligible minimal risk instances of noncompliance, and the RE reviews the log according to the schedule established by the RE. The schedule would begin at least once every three months when the registered entity begins self-logging, which the RE could extend to six months if it deems appropriate.

REs report that registered entities usually include sufficient information in the initially submitted logs, and the REs generally require minimal resources to review logged issues before submitting them to NERC as CEs. This is continuing to improve as registered entities gain experience with assessing the risk of noncompliance, the type of minimal risk noncompliance to include on their self-logs, how to log multiple instances of noncompliance with the same Reliability Standard and Requirement, what information is needed, and how to describe mitigating activities.

There are some instances where REs may request follow-up information from registered entities. These requests can be for information that is included in the templates, like dates to support noncompliance durations and additional details describing the scope of the noncompliance. Based on the type and frequency of missing information, registered entities should consider using the checklists and guidance provided in this user guide when filling out the log.

To maintain the efficiencies of the fast-track disposition of minimal risk noncompliance and keep administrative processes to a minimum, ideally the REs and NERC would only need to do a limited review or editing of logs before posting as CEs. This would also benefit registered entities by not having to revisit facts for a minimal risk noncompliance once submitted.

This report provides considerations for registered entities in completing self-logs. In implementing best practices, it is not the goal that the self-log be lengthy, as it can and should be concise; however, the log must be complete and accurate.

General Guidelines

The Log Should Tell a Complete Story

The reader of the self-log should be able to understand the complete story and not be left with open questions. There should be a direct relationship between the cause of the noncompliance, the minimal risk posed to the BPS, and the mitigating activities. The listed cause of the noncompliance should be consistent with the facts of the noncompliance, the risk it posed, and the actions that are taken to mitigate and prevent recurrence.

Use the Log as a Log

Many registered entities in the program are uncertain whether they should log each instance of noncompliance as it happens, or whether they should, before submitting to their RE, roll up instances of noncompliance of the same Reliability Standard and Requirement together in one line. The preference is for registered entities to be able to use the log as a log – meaning enter each instance of noncompliance as it is identified. The RE would then consolidate as appropriate as it transfers the logged items into the CE template.

Description of the Noncompliance

An adequate self-log includes a description of the facts, circumstances, and scope that is robust enough for the RE, NERC, and FERC to understand what happened, why it happened, and how the registered entity identified there was a noncompliance. The descriptions in the log do not have to be lengthy but do need to include the pertinent information. Attachment B includes example spreadsheets containing points to consider and include if relevant. Attachment C includes examples of self-logs that include a complete picture. Additionally, depending on the

Reliability Standard and Requirement, the REs may also provide additional guidance on what information they prefer to be included. The log should be as concise as possible while being complete.

The registered entity should include the following basic information related to the noncompliance. The information may be included in the description of the noncompliance section, the mitigation section, or as a separate column in the self-log template depending on the circumstances:

- Registered entity name as it appears on the NERC compliance registry (NCR);
- Registered entity's NCR number;
- Registered functions applicable to the noncompliance;
- If an MRRE not in the Coordinated Oversight Program, other affiliates and REs potentially impacted;
- Reliability Standard and Requirements or sub-Requirements as applicable. The correct version of the Standard is based on the start date of the issue. The entity should include the earliest mandatory and enforceable version applicable based on the start of the duration of the noncompliance;
- Date the noncompliance began and an explanation of that date. Ex. July 1, 2016, when the Standard became mandatory and enforceable;
- Date the entity identified the noncompliance;
- Date the noncompliance ended, or is expected to end, and an explanation of that date (e.g., August 5, 2017, when the entity completed its verification settings, or August 5, 2017, when the entity completed its mitigating activities); and
- Date the mitigating activities were completed, or are expected to be completed, including activities to address the cause and prevent recurrence.

In the description of the noncompliance column, the entity should include detailed information, such as:

- An explanation of how the entity discovered the noncompliance, including whether and how its detective controls led to the discovery of the noncompliance;
- The nature and scope of the noncompliance;
- The cause and any contributing factors of the noncompliance;
- Whether the noncompliance was related to management, documentation, performance, training, tools, or some combination;
- The size, nature, criticality, and location of the facility or assets where the noncompliance occurred;
- The system conditions when the issue occurred;
- Whether the noncompliance was isolated or a systemic/general control failure potentially impacting multiple processes/systems; and
- Any internal controls that mitigated or reduced the likelihood of potential harm posed by the noncompliance.

Identifying the Scope of a Noncompliance

Before submitting its log, the registered entity should determine whether conducting an extent of condition review is necessary to determine the full scope of the noncompliance. If the registered entity determines that performing the extent of condition review would prevent notifying the RE during the next log submittal, it would be best to contact the RE for guidance. As self-logged noncompliance should pose no more than a minimal risk to reliability, understanding the scope of the noncompliance is paramount to including it on the log. The registered entity should provide information on the scope of the noncompliance (e.g., number of affected employees, devices, intervals, and

relevant portion thereof). For example, if the noncompliance centers on a Microsoft patch, then the scope may be all facilities that include Windows 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.

Registered entities in the program should understand how broad an extent of condition review should be—and be able to explain that breadth in its log. Depending on the nature of the noncompliance, a registered entity should consider as a part of its scope identification: procedures, assets, facilities, and personnel that are directly affected or could be affected as part of the noncompliance. A best practice for scope consideration is to identify possible risks from not just the instance of noncompliance, but of the identified root cause and contributory causes.

Identifying the Root Cause and Contributing Causes of Noncompliance

Registered entities must conduct a thorough analysis to identify the cause of each instance of noncompliance. The listed cause of the noncompliance should be consistent between the facts of the noncompliance, the risk it posed, and the actions that are taken to mitigate and prevent recurrence. There are many methods that can be used to determine contributing cause(s) of noncompliance without requiring a formal Root Cause Analysis. The guidance, "Cause Analysis Methods for NERC, Regional Entities, and Registered Entities," is designed to provide a reference of the methods and tools routinely used in the investigation, analysis, and determination of causal factors that lead to identification of root cause and contributing factors that lead to noncompliance. Registered entities may use this guidance document along with any other available information to establish a cause analysis methodology.

The registered entity should identify and include in its log all contributing causes of the noncompliance. Cause analysis solves problems by attempting to identify and correct the causes of events (ex. weak key control and training of contractors), as opposed to simply addressing their symptoms (ex. taking away the contractor's key). By focusing correction on causes, the chance of recurrence can be reduced. The cause analysis should be performed by the registered entity for all noncompliance, no matter the discovery method. The cause analysis should tie directly to the mitigating activities included in the log. In this example of a weak key control, the registered entity should consider digging deeper. For example, 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 merger. Why did the old system remain in place? Why were controls different for contractors? And so on.

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

Some suggestions on how to approach determining causes are to first clearly state 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:

- What was the sequence of events that led to the issue?
- Why did the issue develop as it did?
- Is the sequence of events logical? Does it represent an accurate picture of what happened?
- Is this issue a symptom of a potentially larger problem?
- With respect to the cause of the noncompliance, were there extenuating circumstances?

Best practices include doing additional analysis of an initial finding of a human error-based root cause. People make mistakes, but individual behavior is typically influenced by organizational processes and values. The majority of human error-caused noncompliance may be traced to failures in management, tools, or programs/ procedures. This is because humans are fallible, and internal controls should be designed to consider those. Performing a quality cause and control analysis will provide the inputs to design robust mitigating activities, including instituting internal controls that prevent recurrence.

Duration of the Noncompliance

The log should also include the duration of the noncompliance, including start and end dates, and explanation for those dates, if known. For example, a description of duration for a noncompliance may read, "the noncompliance started on July 1, 2016, the day the Standard and requirement became mandatory and enforceable, and ended August 1, 2016, when the entity completed its mitigating activities."

Description of the Noncompliance Checklist

Entities in the Self-Logging Program may find the following checklist helpful to ensure submittals include all pertinent information for CE processing:

- Does the log describe the discovery of the noncompliance?
  - How did the entity discover the noncompliance and how long after the noncompliance began was it discovered? Was it discovered by an employee, manager, security personnel, etc.?
  - Did the entity discover the noncompliance due to an internal review?
  - When was it discovered?
  - What period elapsed between identifying and logging the noncompliance? If there is an extensive gap beyond the logging period (i.e., more than three months), explain.
  - Has the same noncompliance been logged or reported previously to the same or other REs?
- Does the log describe the noncompliance?
  - Does the log include the Reliability Standard and Requirements at issue?
  - Is the noncompliance adequately described by tying the description to the Reliability Standard?
  - Does the description include what happened?
  - Was an extent of condition review performed, and if so, does the log include a description of what other procedures, assets, facilities, or personnel were impacted or could be impacted by the noncompliance?
- Does the log describe the cause of the noncompliance?
  - Has the root cause been identified and included?
  - Were there any contributing factors identified? If so, were they also included?
  - Did the entity review its detective processes to determine if anything needs to be improved or implemented?
- Does the log include duration information along with the explanation of start and end dates?

Description of the Risk

A best practice in describing the risk is to frame the discussion in three parts. First, the entity should describe the potential for harm to the reliability or security of the BPS under the facts and circumstances of the noncompliance. Second, the entity should describe what factors were in place that mitigated or reduced the potential for harm—by reducing the magnitude of the harm or the likelihood of the harm occurring. Third, if the mitigating activities are not

complete when the registered entity submits its log, then the entity needs to include a discussion of its interim risk reduction. Specifically, this means the registered entity must include the steps it is taking to reduce or eliminate risk to the BPS while implementing its mitigating activities.

Only issues with a minimal risk to the reliability of the BPS are eligible for self-logging. Issues that are determined to be a moderate or serious risk, or issues that relate to or involve any of the following: 1) extended outages; 2) loss of load; 3) cascading blackouts; 4) vegetation contacts; 5) systemic or significant performance failures; or 6) intentional or willful acts/omissions and gross negligence or other misconduct, are not eligible for inclusion.

If the registered entity is not certain about the level of risk associated with a specific noncompliance, the registered entity should contact the RE to discuss the noncompliance and determine whether it is appropriate for logging as a minimal risk issue. In the event the registered entity identifies noncompliance and determines that it poses more than a minimal risk or is not certain of the level of risk posed by the noncompliance, the registered entity would instead self-report the noncompliance to its RE.

Description of the Potential Harm

The registered entity should provide details about what harm might have resulted from the noncompliance at the time it took place. The registered entity's description of the possible harm should consider, when applicable, the following:

- Whether the noncompliance is limited to an administrative or documentation error;
- The size and interconnectedness of the particular registered entity;
- The impact the noncompliance could have had under different circumstances;
- The location or asset involved with the noncompliance; and
- The status of the BPS when the noncompliance occurred (e.g., extreme weather, outages, islanding, etc.).

Description of Mitigating Factors that Reduce the Magnitude or Likelihood of the Harm

The registered entity should determine what factors were in place that mitigated or reduced the potential for harm to the BPS. The analysis may include, if relevant, identifying the short duration or limited scope of the issue, internal controls (preventive, detective, and corrective), or redundant equipment (backups or other entities performing same function) in place when the noncompliance occurred. Other considerations may include the following:

- The timeliness of detection.
- The method of detection (e.g., whether detection is the result of effective execution of internal controls), and
- A description of the controls in place that shortened the duration or reduced potential harm of the noncompliance. Examples could include alarming, redundant systems, security perimeters, firewalls, CCTV, etc.

The registered entity should assess its own prior compliance history of similar conduct, if known. Although prior compliance history is not necessary to include in the log, it could inform mitigating activity design or alternatively, could potentially increase the risk posed by a noncompliance—voiding the appropriateness of self-logging treatment.

Interim Risk Description

If the mitigating activities required to end the noncompliance are not complete when the registered entity submits its log, then the registered entity must include a discussion of its interim risk reduction. The registered entity must include steps that will reduce or eliminate the risk to the BPS posed by the noncompliance while mitigation is being implemented. This step is especially critical for activities with longer durations. In determining interim actions and

activities, registered entities should identify and address any risks to the BPS posed by the noncompliance 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 those risks. The discussion should include actions or processes in place during the noncompliance that mitigated the risk or acted as a meaningful correction to the instance of noncompliance; and the timing and level of efforts undertaken, or to be undertaken, to mitigate the noncompliance.

Risk Description Checklist

Entities in the Self-Logging Program may find the following checklist helpful to ensure submittals include all pertinent information for CE processing:

- Is there a discussion of the system conditions during the noncompliance, if relevant? For example, did the noncompliance take place while the system was stressed or during extreme weather events?
- Does the risk address the size, nature, criticality, and location of the facilities at issue or other entity facilities potentially affected?
- Are the circumstances surrounding the noncompliance rare or common?
- Does the risk statement discuss the controls in place to identify the noncompliance and prevent risk to the reliability of the BPS?
- Is there an explanation of any extensive duration of the noncompliance before discovery? If so, does the risk statement include a discussion of what controls were in place during that time to prevent harm?
- Does the risk statement account for the risk posed by the root cause or contributing causes?
- If the mitigating activities required to end the noncompliance are not complete when the registered entity submits its log, is there a discussion of its interim risk reduction?

Description of Mitigating Activities

Mitigating activities are sets of tasks developed by a registered entity to: 1) correct noncompliance with a Reliability Standard; 2) address the root cause of the noncompliance; and 3) prevent recurrence of the noncompliance. Registered entities' logs should include a comprehensive description of any mitigating activities that have concluded or are in progress.

Mitigating activities should take prevention of harm into account. This is to ensure that the root cause of the noncompliance is addressed and the future risk will continue to be minimal.

Best practices include considering how the successful completion of the included mitigating activities prevent or minimize the probability that the organization would have noncompliance with the same or similar Reliability Standards requirements in the future.

Best practices for registered entities in the program are to be as complete, yet concise, as possible with the description of mitigating activities within the self-log and not subsequently submit a formal Mitigation Plan unless requested to do so directly by the RE. Formal Mitigation Plans have specific timing considerations that apply per Section 6 of Appendix 4C of the NERC Rules of Procedure and should be restricted to activities taking longer than a year to perform, higher risk instances, etc., any of which could remove eligibility of the noncompliance for inclusion on a log.

Corrective Actions

Corrective actions should be designed to mitigate 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. Best practices would include ensuring onboarding training of new personnel as well as requiring recurring training. Lack of training should rarely be considered a root cause, therefore training a single individual or group of individuals will rarely be adequate alone for mitigation, as noncompliance is likely to recur after personnel turnover.

Preventive and Detective Actions

Preventive and detective actions should detect the noncompliance in advance and prevent it, reduce the duration, or reduce the likelihood of recurrence. When identifying these actions, the registered entity should focus on both procedural and technical internal controls that may be available to help detect and prevent future occurrences. Addressing the cause and any contributing factors with controls to prevent and detect will generally lead to effective and sustainable mitigation.

Compliance History Consideration

A registered entity should not include its compliance history within the self-log. Nevertheless, best practices would include reviewing its, and its affiliates, if applicable, compliance history to see if the current issue has occurred previously. This identification will provide information on the success of past mitigation. If the registered entity has multiple instances of noncompliance with the same Reliability Standard/Requirement, with the same or similar root causes or conduct, there may be an underlying issue that the registered entity has not identified or fully addressed.

Relevant compliance history includes, but is not limited to, the following:

- Prior noncompliance with same/similar Standard for the entity at issue,
- Prior noncompliance with same/similar Standard for affiliates, and
- Prior noncompliance with same/similar Reliability Standards in other REs when there is a commonality of compliance responsibility between the entity/affiliates, and compliance history indicating broader programmatic failures (e.g., multiple CIP violations may indicate a failure of the entity's CIP Compliance Program).

Mitigating Activities Checklist

Entities in the Self-Logging Program may find the following checklist helpful to ensure submittals include all pertinent information for CE processing:

- Do the activities address the scope of the noncompliance being mitigated?
- Do the activities address each of the contributing factors and causes of the noncompliance?
- 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 before submission of the activities been included? If not, does the log include a proposed completion date?
- If not completed when submitted, do the activities address the interim risk associated with the reliability of the BPS while the activities are being implemented?
- Do the activities describe the prevention of future risk to the reliability of the BPS?
- Do the activities describe how the successful completion of these activities prevent or minimize the probability that your organization incurs further risk of noncompliance with the same or similar Reliability Standards requirements in the future?

Avoid Inclusion of Confidential, Privileged, or Critical Energy/Electric Infrastructure Information

The ERO Enterprise has identified universal best practices for avoiding the inclusion of confidential information when registered entities are drafting self-logs. Although logs should describe the nature and extent of the noncompliance, registered entities should avoid unnecessarily identifying any critical energy/electric infrastructure information (CEII)[16] within non-CIP logs. For best practices, the logs should do the following:

- Not include any individual employee/contractor/etc. personal names;
- Avoid CEII unless necessary to understand the nature or extent of the noncompliance;
- When possible, refer to "the entity" instead of using the entity's name or acronym in the main body sections;
- Avoid using upper case names or titles—these are more likely to be entity-specific and require redaction for the public posted version; and
- Avoid using entity-specific acronyms:
  - Cyber Vulnerability Assessment (CVA) is an example of language of a common acronym or language found in Reliability Standards.
  - Unit Theta Back-up Control Center (UTBCC) is an example of an entity-specific acronym that should be replaced with a more generic "control center."

[16] For a discussion and description of "CEII" under FERC regulations, see https://www.ferc.gov/legal/ceii-foia/ceii.asp.

Chapter 4: Maintaining a Record

For each instance of noncompliance recorded on the log, the registered entity must maintain evidence to support the details included in the description of the noncompliance, the minimal risk assessment of the noncompliance, and the completion of mitigating activities. Although a formal certification of completion is not required for mitigating activities, the registered entity should still inform the RE that activities are complete and the date those activities were completed as soon as practicable after completion.

The registered entity shall maintain this evidence until the RE verifies completion of the mitigating activities, subject to the following exception: If the RE has not verified the completion of the mitigating activities within 18 months from the later of the date the RE sent the Notice of CE treatment or the date the registered entity completes the mitigating activities, the registered entity is no longer required to maintain the evidence.

Verification Sampling of Self-Logged Noncompliance

The ERO Enterprise is working to develop guidelines to be used for verification of completed mitigating activities for CEs. Self-logged noncompliance, by definition, are minimal risk, and REs could likely better focus their time and energy on other matters instead of verifying completion of mitigation for all self-logged items.

Accordingly, the REs may have a sampling program to select noncompliance for verification. For sampling of self-logged noncompliance, the RE will notify the registered entity and identify the logged noncompliance for which mitigating activity is being verified.

After this notification, the registered entity will submit evidence supporting mitigating activity completion to the RE. The evidence submitted by the registered entity will be reviewed by the RE. The RE will maintain a record of the evidence reviewed to verify completion of mitigating activities. The RE will notify the registered entity upon verifying completion of mitigating activities.

If the RE has any issues with the evidence submitted by the registered entity, the RE will seek to resolve those issues with the registered entity. Where the verification reveals a pattern or practice of lack of mitigating activity completion or poor record keeping, the RE may modify or revoke the registered entity's self-logging eligibility. If the RE does so, it will inform the registered entity and NERC of the basis for that decision.

Chapter 5: Conclusion

As a direct benefit from the Self-Logging Program, registered entities have gained experience, received expedited treatment and easier reporting, and demonstrated their capability to focus on reliability and manage risk. REs have streamlined processing, reduced their caseloads, and enhanced the efficient resolution of noncompliance.

To realize the benefits of this program and to support future growth, registered entities should continue to seek entry into the program. RE outreach to registered entities about the requirements, process, and benefits of the program to encourage participation is paramount. In addition, registered entities need to have the requisite information and abilities to provide complete and accurate logs, as discussed in this user guide.

This guide provides additional support and guidance to improve registered entity submissions and reduce the need for REs to request additional information. The guide supplements information provided in the NERC CMEP, Rules of Procedure, Appendix 4C, and the Self-Report and Mitigation User Guide.

Appendix A includes a sample eligibility spreadsheet checklist.

Appendix B includes a step-by-step walkthrough of a Self-Log template.

Appendix C includes examples of self-logged noncompliance with robust descriptions, risk assessments, and mitigating activities.

Appendix D includes RE-specific resources for additional information or to request eligibility review for entry into the Self-Logging Program.

Appendix E includes additional FERC and NERC resources for registered entities interested in the Self-Logging Program or risk-based compliance monitoring and enforcement generally.

Appendix A: Eligibility Checklist

The below checklist includes examples of narratives or evidence an entity could provide to show it has the capability to timely identify, assess, and correct noncompliance. The list is not intended to be exclusive and could be expanded or reduced depending on the registered entity. Registered entities should refer to the below as elements to include in the narratives or evidence they submit to the RE during eligibility review.

Evidence or narratives of the registered entity's established or formal internal controls or compliance program:

- Copies of formal or established compliance programs related to NERC Reliability Standards:
  - Evidence the program grants authority and responsibilities for compliance,
  - Evidence of version control, and
  - Evidence of a senior officer signature, title, and date page.
- The compliance program, or other programs supporting compliance activities, identifies when, where, and to whom it was disseminated;
- Links to the compliance program website or internal corporate site where employees have access:
  - Signature of annual review by employees, etc.
- Clearly identified oversight position, along with the responsibilities and requirements of a compliance official. Evidence the oversight position is supervised at a high level in the entity;
- An organizational chart that clearly identifies compliance program responsibilities;
- Clear description of how senior management is involved;
- Company policies regarding compensation, promotion, and disciplinary action take into account compliance with approved Reliability Standards and the reporting of any violations;
- Meeting schedules on compliance matters (new standards, Self-Certifications, Audits, Internal Assessment status and results) on a monthly or other specified basis;
- Use of other departments such as Human Resources, Legal, or Internal Auditing to operate or manage the program;
- Use of other outside sources such as other related facilities or plants; and
- Explanation of the resources for the entity related to its compliance program. Examples could include:
  - Identifying the portion of the entity's resources that are dedicated to the compliance program, and
  - Indicating that the compliance program funding is managed independently.

Evidence the entity identifies and mitigates noncompliance in a timely manner:

- Detective controls, reviews, internal audit schedules, external consultant reviews, etc.;
- Narrative or established program describing cause and controls analysis process, requirements for investigation teams, success, etc.;
- Evidence the registered entity adopts new and effective internal controls to prevent recurrence of noncompliance;
- Attendance at RE or ERO standards and compliance workshops, independent training events related to NERC reliability, standards, or compliance;
- Compliance history, number/risk/timely mitigation;

- Frequency of timely and accurate Self-Reports. The number or frequency of RFIs required for the RE to understand the scope, risk, cause, etc. of the noncompliance;
- Frequency of timely mitigation. History of needing milestone or Mitigation Plan extensions;
- History of mitigation to correct the noncompliance and prevent recurrence being of high quality and thorough;
- Documentation that includes a description of self-assessment and steps (or controls) to keep noncompliance from occurring again; and
- Documentation of a provision for how to identify weakness and how to strengthen the weakness.

Appendix B: Self-Log Template Walkthrough

Name of Entity	NCR Number
The registered entity name and NCR number should appear exactly as on the NERC Compliance Registry Matrix, available here: https://www.nerc.com/pa/comp/Pages/Registration.aspx	

MRRE Only–Region(s) Impacted
MRREs in the Coordinated Oversight Program: The registered entity should include its Group Name, Group Number, all other RE footprints in which it maintains a registration affected by the self-logged issue, the affected NCR IDs, and the affected NCR ID names. MRREs not in the Coordinated Oversight Program that are logging a noncompliance relevant in other RE footprints or for affiliates or other related entities: The registered entity should include all other RE footprints in which it maintains a registration, and the NCR IDs for affiliates not in Coordinated Oversight.

Standard and Requirement(s)
The version should be the applicable Reliability Standard and Requirement that was mandatory and enforceable at the start of the duration of the noncompliance. All requirements and sub-requirements should be listed if applicable. If a noncompliance involves more than one requirement sub-requirement, they may all be listed together. If a noncompliance involves more than one Standard or Requirement, they should be logged as separate issues.

Date Noncompliance Started (for more than one instance, use earliest date)
Dates should be listed in X/XX/XXXX format and include an explanation for that start date. For example: 7/1/2016 (when the Standard became mandatory and enforceable for Entity).

Date Noncompliance Ended (for more than one instance, use latest date)
This should be the date of the expected end, or actual end of the noncompliance if complete, (for more than one instance, use latest date). Dates should be listed in X/XX/XXXX format and include an explanation for that end date. For example, 6/1/2016 (when Entity completed all mitigating activities). This date is not necessarily tied to the mitigating activities completion date. If a specific action brought the registered entity back into compliance before the mitigation completion date, the earlier date would be the appropriate choice.

Expected Mitigating Activities Completion Date
This should be the date of the expected or actual completion of mitigating activities.

Description of How the Entity Identified the Issue
Describe how and when the noncompliance was discovered. Was it discovered by an internal employee or by a third party? Was it discovered through self-evaluation, internal review or investigation, or the internal compliance program?

Description of the Noncompliance

Describe what happened: why it happened (cause); where it happened (type of Facility, location of Facility, etc.); and how it happened (facts and circumstances surrounding the noncompliance). This should include identification of the nature and scope of the noncompliance, which includes but is not limited to, number of affected employees, types of affected systems (e.g. relays, CTs/PTs, batteries, etc.), and number of devices and descriptions, intervals, and relevant portion thereof.

Cause of the Noncompliance

Describe the contributing cause(s) of the noncompliance. Each instance of noncompliance requires the cause(s) to be identified within the log. The listed cause(s) of noncompliance should be consistent between the facts of the noncompliance, the risk(s) it posed, and the actions taken to mitigate and prevent recurrence.

Potential Impact or Harm

Include a discussion of the potential harm as relevant to the entity and circumstances; do not include a blanket heightened risk statement related solely to the Standard (R) at issue. For example, the potential impact posed by a 15 MW wind facility and a 500 MW coal-fired facility should be different. Elements to consider may be size or location of the facilities, interconnections, miles, and kV of transmission lines, etc.

Likelihood of Impact/Justification of Minimal Risk

Include a description of elements reducing the likelihood of harm occurring, including internal controls, systems, and processes in place to prevent escalation. If the noncompliance is still ongoing, include factors or controls that are reducing the risk during the interim.

Description of Mitigating Activities to Resolve Noncompliance

Include the activities taken to resolve the noncompliance. Also include immediate actions taken before self-logging; for example, if the entity revoked access for an individual, checked remaining devices, etc.

Description of Mitigating Activities to Prevent Recurrence

These activities should correspond directly to the identified causes of the noncompliance. If there are commonalities in cause or conduct with those of a prior noncompliance, this information should be used to identify additional activities to prevent further recurrence.

Appendix C: Self-Log Examples

Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Transmission Owner (TO), was in noncompliance with FAC-008-3 R8.1. Specifically, Entity failed to provide requested information of a planned upgrade to its Planning Coordinator or Reliability Coordinator (PC/RC) at least seven business days before the expected in-service date, as specified in the PC/RC's Reliability Analysis Data Manual. The planned upgrade consisted of increased thermal ratings for a 115 kV feeder, which resulted from a change in bus work. This noncompliance began on January 1, 2017, one day after the required date for submittal of the information to the PC/RC, and ended on February 3, 2017 when the Entity submitted the information. The root cause of this instance of noncompliance was the lack of controls surrounding its protocol related to updating Facility and Equipment Ratings. While there was a protocol in place, there were no checks to ensure the department responsible followed that protocol.	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. As neither the PC/RC nor the Entity's own system operators were timely informed of the increased facility ratings for the transmission line, the transmission system continued to be operated to the lower existing ratings during the one month period of noncompliance. In addition, the lapse occurred during the winter operating period. Entity is a summer-peaking utility, therefore its customer loads during the period of noncompliance are greatly reduced, thus offsetting the impact of the failure to use higher ratings for a single transmission feeder. Entity performed a review of its related protocols and changes (approximately 20 changes) for the prior two years and identified no other instances. No harm is known to have occurred as a result of this noncompliance.	To mitigate this issue, Entity corrected the noncompliance by providing the required information submittal to its PC/RC. To prevent a recurrence of similar instances of noncompliance, Entity created process documents to formalize the existing monthly review processes that the relevant departments follow with respect to Facility and Equipment Ratings. Each process document is aligned with the structure, job titles, responsibilities, and review activities within the Entity's RCs' footprints. Training on the changes was provided to responsible staff. Training included an after-action review and creation of a best practices document. A new onboarding training was created as a part of its process document to ensure new personnel are aware of responsibilities. Entity completed these activities on April 10, 2017.
Entity, as a Distribution Provider (DP) and Transmission Owner (TO), was in noncompliance with CIP-004-6 R3. Entity failed to conduct a Personnel Risk Assessment (PRA) for one individual with authorized unescorted physical access within seven calendar years of the previous PRA completion date. The Entity's process included a trigger for checking PRA status in the administrator's calendar on a monthly basis. The individual's PRA expired in the week after she was granted unescorted physical access. Therefore, her PRA was current when access was granted but the next review occurred after the PRA expired. The noncompliance duration was approximately three days and began on January 1, 2017, the day after seven calendar years of the previous PRA, and ended on January 3, 2017, when the entity revoked the individuals' unescorted physical access. The root cause of the noncompliance was a gap in the entity's process for identifying PRAs that are expiring soon after granting unescorted physical access rights.	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, the individual is an employee who has worked with the entity for 13 years and is still currently employed by the entity. The employee had a prior PRA and up-to-date CIP training. The individual further did not have electronic access rights to the BES Cyber Systems. Additionally, the individual's PRA was renewed on February 1, 2017, with no adverse findings. The individual in scope had access to 45 Physical Security Perimeters (PSPs) classified as Medium impact facilities. During the three-day period where the PRA had lapsed, the individual in scope did not access any PSPs. No harm is known to have occurred.	To mitigate the issue, the entity: 1) Revoked unescorted physical access for the individual in scope; and 2) Performed a PRA on the individual in scope. To prevent recurrence of the issue, the entity updated its Corporate Security procedures to notify its internal compliance group when access is granted and the PRA for the individual will expire within the next six months. Entity completed these activities on March 3, 2017.

Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Transmission Service Provider, was in noncompliance with MOD-030-2 R10. Entity did not recalculate the Available Flowgate Capability (AFC) for hourly AFC and daily AFC as required. Entity relies upon its Reliability Coordinator (RC) and a third-party independent transmission organization (ITO), which provides independent transmission tariff administration services to Entity, to calculate AFC and post Available Transfer Capability (ATC) on behalf of Entity. On September 1, 2016 at approximately 12:00 p.m., the RC's File Transfer Protocol (FTP) process that uploads the latest AFC initial values and the Transfer Distribution Factors to the program on an hourly basis failed. As a result, the tool used old data to calculate AFC and ATC for hourly and daily values. The ITO's hourly ATC calculation was incorrect for approximately 270 hours for purposes of MOD-030-2 R10.1. The ITO's daily ATC calculation was incorrect for 4 days for purposes of MOD-030-2 R10.2. The failure did not affect monthly calculations. On September 5, 2016, the ITO discovered the noncompliance during its AFC verification process. The ITO verification process is an internal control that the ITO implemented to identify any issues in the AFC calculation process. The internal control the ITO had in place was a manual checklist that included a step requiring the ITO to verify the date of the file. The ITO was required to complete the checklist verification on a daily basis, but the ITO failed to perform the review daily. Therefore, the ITO did not identify the noncompliance for several days. The cause of this noncompliance was the failure of the FTP process that uploads the latest AFC values and the failure of the ITO's internal controls to detect the failure of the FTP process. This noncompliance started on September 1, 2016, when Entity began incorrectly calculating hourly and daily ATC and ended on September 5, 2016, when Entity began correctly calculating hourly and daily ATC.	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Entity's failure to recalculate AFC for hourly and daily AFC could have led Entity to erroneously approve or refuse, and subsequently schedule or not schedule, a transmission service request based on posted incorrect ATC values, which could contribute to system overload. Nevertheless, if Entity had erroneously approved transmission service requests, the Balancing Authority (BA) and RC have other tools, such as Transmission Loading Relief (TLR) or redispatch, to allow them to identify and mitigate any operating issue that may have arisen. If Entity had erroneously refused and prevented a load-serving entity from importing needed energy, the BA carries appropriate operating reserves (approximately 2,800 MW). Entity's review of operations confirmed that no TLRs or operational issues occurred during the noncompliance. In addition, Entity determined that the correct AFC information would not have changed its decisions to accept or reject transmission service requests during the noncompliance. No harm is known to have occurred. Neither the Entity nor any of its affiliates have relevant compliance history.	To mitigate this noncompliance, Entity correctly calculated the hourly and daily ATC. To prevent recurrence, the RC implemented an alarm that alerts Entity when the FTP process fails to upload current data. In addition, Entity had the ITO add a schedule reminder and a requirement to its daily AFC checklist that includes the RC's FTP file list showing the update date and time. These activities were complete on October 5, 2016.

Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Balancing Authority (BA), was in noncompliance with TOP-002-4 R7. Entity did not provide its Operating Plans for next-day operations identified in Requirement R4 to its Reliability Coordinator (RC) on two days in June 2017. During its regular monthly review, Entity discovered that it did not send its Operating Plans for next-day operations to the RC on two occasions in the month before. The transmission compliance engineer verifies after the fact that Entity sent the output of the resource monitor to its RC each day of the previous month. When the noncompliance occurred, Entity had internal controls that issued a single reminder alarm on the Energy Management System (EMS) to occur daily at 11:00 AM EST to serve as a reminder to run the resource monitor and send the file to the RC, and notifies the System Operator upon closing the resource monitor tool if it has not been sent to the RC. Entity determined that, although it trained System Operators not to acknowledge the EMS alarm before sending the resource monitor output to its RC, the operational procedure did not specifically instruct the System Operators to send the resource monitor output before acknowledging the EMS alarm. The cause of the noncompliance is insufficient processes and management oversight. This noncompliance occurred on June 1, 2017 and June 2, 2017, when Entity did not send its Operating Plans for next-day operations to the RC.	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Entity's failure to provide the Operating Plans for next-day operations to its RC could result in the RC not being able to fully assess its next-day ability to operate within the System Operating Limits. Nevertheless, the Entity Operating Plan for next-day operations included the next-day forecasted load, generation, and Net Scheduled Interchange data for the Entity BA. In addition to the resource monitoring tool and as a part of daily operations, the RC receives the next-day forecasted load and Net Scheduled Interchange. Therefore, the only information the RC did not receive was the generation component of the Operating Plan for next-day operations. The RC is aware of any generation that is unavailable or de-rated via System Operator submission to the RC Coordination website. The RC assumes that any generation not submitted as an outage into the RC portal is either in service or readily available for use. According to Entity, the RC verified and confirmed there were no reliability issues on June 1, 2017 and June 2, 2017 as a result of not receiving Entity's BA Operating Plans for next-day operations. No harm is known to have occurred.	To prevent recurrence of this noncompliance, Entity: 1) Set the Windows task scheduler to automatically initiate the resource monitor tool at 10:45 A.M. daily to serve as a reminder that the resource monitor must be run daily; 2) Established an email reminder notification that occurs daily at 1:00 P.M. EST to serve as a final reminder to run the resource monitor and send to the RC; 3) Updated the procedure to note that the resource monitor output must be sent to the RC before EMS alarms can be acknowledged; and 4) Reviewed the updated procedure with all operators and added the requirements to the onboarding and annual trainings. Entity completed these activities on August 15, 2017.

Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Transmission Owner and Transmission Operator, had an issue with CIP-007-6 R5. Specifically, Entity did not implement one or more documented processes that included Part 5.2 on an EACMS server. The Entity uses multiple interfaces to review its assets on a periodic basis. On December 4, 2016, the Entity discovered a previously unidentified and un-inventoried default generic account on the EACMS server. The Entity discovered the account was not visible during the initial scan when an analyst used a graphical user interface (GUI), but was visible during a subsequent review when a different analyst used a command line interface. The EACMS server is associated with a medium impact BES Cyber System. The EACMS server was used for application discovery and dependency mapping. Entity ran both a GUI and command line interface to ensure it had identified and inventoried all known enabled default or other generic account types and identified no other inaccuracies. The cause of the noncompliance was that Entity failed to realize relying on GUI is insufficient and would not identify all of the accounts that were present on the device. The noncompliance began on July 1, 2016, when the standard became mandatory and enforceable, and ended on August 4, 2016, when the account was inventoried, approximately one month later.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Entity tracks approximately 2,000 default and shared accounts, meaning this noncompliance involved less than .05% of its accounts. In addition, the device at issue uses dual-factor authentication for electronic access that would have prevented most forms of unauthorized electronic access. A review of system logs did not identify attempts to access the account before Entity identifying and mitigating the noncompliance.	To mitigate this issue, Entity inventoried the account. To prevent recurrence of this noncompliance, Entity: 1) Conducted an extent of condition analysis and confirmed the noncompliance was limited to the single default generic account; and 2) augmented its procedures to conduct future assessments using both GUI and command line interface. Entity completed these activities on December 1, 2016.

Description of the Noncompliance	Description of the Risk	Description of the Mitigation
Entity, as a Transmission Operator was in noncompliance with CIP-006-6 R1. On January 20, 2018, a contractor worked at a substation removing material from the substation via a door to the street. During the pre-job briefing, the contractor was informed by the Entity permit holder that the contractor was not permitted to exit the facility in this manner without the permit holder in attendance. In the morning, members of the contractor crew were removing material through the door with the permit holder in attendance; however, during a half-hour period beginning 10:00 a.m. on the 20th, the contractor opened the door and was removing material without the permit holder in attendance. The contractor was approached by an Entity field planner who was passing by the substation and observed the open door. The field operations planner stopped the work and notified the permit holder. The substation is a medium impact facility for cyber security compliance and the door in question is a perimeter access point. CIP-006-6 R1 requires the Entity to document and implement a plan to restrict access to BES Cyber Systems. The Entity plan stipulates that leaving an opened access point unattended is prohibited. On January 20th, for a half-hour, evidence indicates that the substation door was open and unattended by the permit holder. Video records confirm that the contractor periodically entered and exited via the door while removing material from the substation. There were periods, lasting up to five minutes, where no one was visibly present at the open door. The root cause of the noncompliance was the failure of the contractor to follow clear directions from the permit holder and failure to ensure an Entity permit holder was available continuously or was able to secure the door when absent. The issue began on January 20, 2018 when the perimeter access point was left unattended and ended thirty minutes later on the same day when an Entity employee resolved the issue.	This noncompliance posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Video records confirm that no one other than contractor and Entity personnel entered the substation via the open door. An Entity employee observed the open door and investigated, facilitating a rapid resolution of the issue. Also, there are additional doors/walls separating the substation BES Cyber Assets from the perimeter access point on the street. Risk was also limited by the short duration that the perimeter access point was open and unattended. No harm is known to have occurred as a result of this issue of noncompliance.	To mitigate this issue, Entity employee closed the door and alerted the permit holder. To prevent recurrence of the noncompliance, the Entity: 1) Logged a complaint against the contractor in its system. The contractor was advised on the issue and the contractor agreed that, on an on-going basis, they will direct their personnel via toolbox talks and pre-job briefings of security procedures and the requirement that no one is to enter/exit without Entity substation personnel escorting them. 2) Revised its CIP-006 Procedure to clarify that an authorized person must be in attendance when a perimeter access point is left open. 3) Sent an email to all substation operations employees stating that contractors shall follow the physical security rules. 4) Held a quarterly meeting with substation employees to discuss the event. 5) Reviewed the CIP-006 issue with executive management at an expanded staff meeting. Entity completed all activities on April 1, 2018.

Appendix D: RE-specific Self-Logging Program Information

- FRCC
  - Self-Logging Page
  - Self-Logging Contact Email Address
  - Self-Logging Procedure
  - Self-Logging Information Document
  - Self-Logging Request Form
- MRO
  - Self-Logging Page
  - Self-Logging Contact Email Address
  - Self-Logging Eligibility Determination Process
- NPCC
  - Self-Logging Page
  - Self-Logging Contact Email Address
- RF
  - Self-Logging Policy and Procedure
  - Self-Logging Request Form
- SERC
  - Entity Request for Evaluation of Eligibility for Self-Logging Privileges
  - Self-Logging Contact Email Address
  - Procedure for Self-Logging Minimal Risk Instances of Noncompliance
- Texas RE
  - Self-Logging Program Participation Request
  - Self-Logging Contact Email Address
  - Self-Logging Guide
- WECC
  - WECC's Self-logging Program and Criteria Document
  - Self-Logging Contact Email Address
  - Self-Logging Application

Appendix E: General Guidance and Reference Documents

General Guidance and 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

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, (October 26, 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 (October 16, 2008) http://www.ferc.gov/whats-new/comm-meet/2008/101608/M-3.pdf

Revised Policy Statement on Enforcement (May 15, 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 and Reference Documents

ERO Enterprise Self-Report and Mitigation User Guide: https://www.nerc.com/pa/comp/Reliability Assurance Initiative/Registered Entity Self-Report and Mitigation Plan.pdf

Public CIP CE and non-CIP Consolidated Spreadsheets: https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx

Template for Compliance Exceptions and Find, Fix, Track and Report: https://www.nerc.com/pa/comp/CE/Templates/Template%20for%20Compliance%20Exception%20(CE)%20and%20Find,%20Fix,%20Track,%20and%20Report%20(FFT).xlsx

ERO Enterprise Self-Logging Program Document: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Updated_ERO%20Enterprise%20Self-Logging%20Program%20(2-1-16).pdf

Compliance Exception Overview: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf

Cause Analysis Methods for NERC, Regional Entities, and Registered Entities, issued September 2011: http://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/Cause%20Analysis%20Methods%20for%20NERC,%20REal%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

ERO Enterprise Guide for Internal Controls: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf