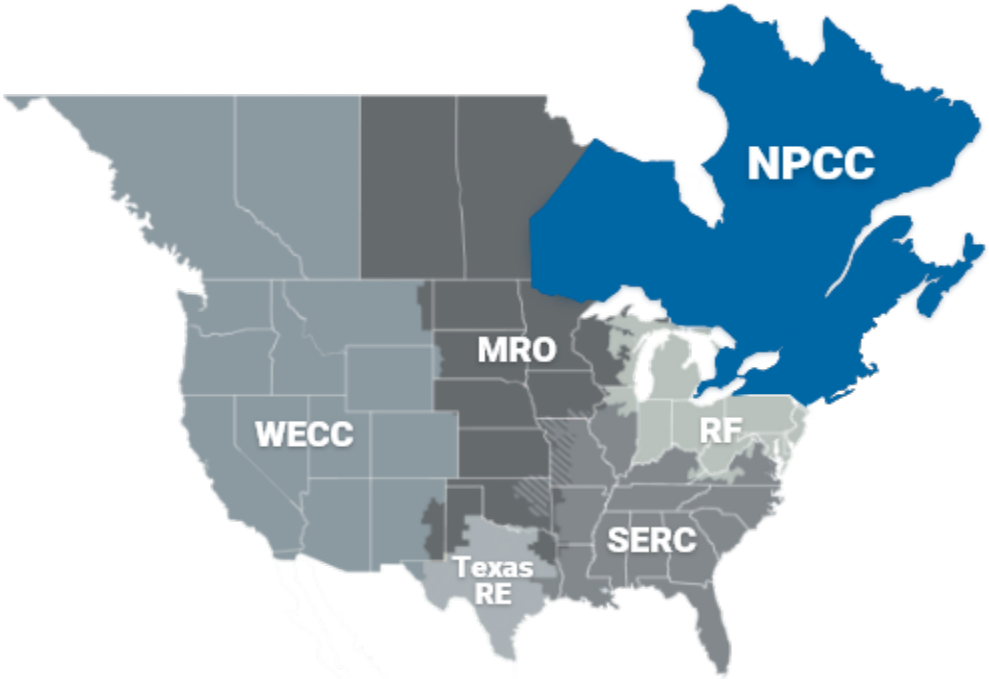
Generator Welcome Package



January 2023

Contents

INTRODUCTION **3**
General Considerations for Generator Owners (GOs) or Generator Operators (GOPs) Preparing for NERC Registration 3
Coordinating NERC Registration 4
Preparing to be Compliant 4
Upon NERC Registration Becoming Effective 5
ERO Compliance Guidance 5
THE IMPORTANCE OF INTERNAL CONTROLS **6**
Preventative Controls 6
Detective Controls 6
Corrective Controls 7
Assessing the Effectiveness of Internal Controls 7
Suggested Reading on Internal Controls 7
GO/GOP DUE DATES FOR ASPECTS OF CERTAIN STANDARDS **8**
INTERNAL CONTROLS CONSIDERATIONS FOR CERTAIN STANDARDS **15**

Introduction

General Considerations for Generator Owners (GOs) or Generator Operators (GOPs) Preparing for NERC Registration

The following package provides a framework to prepare a Generator Owner (GO) and Generator Operator (GOP) for its compliance obligations. With proper planning for establishing and assessing it's state of compliance, an entity is better prepared to be compliant on the effective date of the registration change. NPCC recommends that entities consider the following points when registering a new entity or adding generation to an existing entity.

- ❑ The compliance obligation begins on the day that the registration is made effective with NERC unless a Requirement specifically states or an implementation plan (or other authoritative document) specifies the date by which the entity is required to be compliant. The entity should be audit-ready on the day it is registered with NERC.
- ❑ The entity's Compliance Department should become involved early in the process when bringing a new generator online. Preparing a new GO or GOP for compliance may take 6-12 months of preparation before the NERC registration becomes effective which will depend on the maturity of the existing compliance program. Entities should ensure they have a sufficient amount of time to develop and implement business processes to address the applicable Reliability Standards[1]. Much of the evidence gathering and evaluation, however, will likely occur close to the NERC registration date.
- ❑ Consider developing a method of tracking preparations through the first year after registration to ensure all initial compliance tasks are completed. The GO/GOP Roadmap and Internal Controls Considerations tables in this document tables provide high level timelines, best practices, and recommendations to aid entities in developing a company-specific tracking method.

[1] The Standards referenced throughout this Welcome Package were active Standards when the Welcome Package was posted. NPCC will periodically update the Welcome Package as Standards change.

- ❑ The entity should develop procedures and process documents that define and document the entity's business processes with compliance built in. Entities should refrain from writing generic procedures that reiterate the language in the Standard.
- ❑ Entities are encouraged to establish strong and documented operational business processes with preventative, detective, and corrective internal controls for applicable NERC Reliability Standards and Requirements. The business processes should be designed around the GO's and GOP's needs. For example, COM-002-4 does not require a documented procedure explaining three-part communications training. However, entities should consider establishing processes for identifying new operators who require three-part communications training, conducting training, and tracking training. These processes will be unique to the way the company does business.
- ❑ The tables in the Internal Controls Considerations for Certain Standards section provide best practices and common industry processes and are provided as a guide to help entities when developing internal controls.

Coordinating NERC Registration

NERC Registration is coordinated with the Regional Entity's registration team with the submission of the registration package typically occurring 60 days prior to the planned registration date.

Preparing to be Compliant

When establishing a new Generator Owner, a new Generator Operator, or bringing a new generator online under an existing registration, there are certain activities that should be undertaken prior to the effective date. These activities include developing procedures and processes, establishing and documenting internal controls, completing the commissioning of equipment and Facilities, and performing initial compliance activities where necessary. The entity should further complete its due diligence to understand which Standards are applicable to its NERC registration while also making itself aware of which compliance obligations are due at the effective date of registration, those which are event driven, and those which are time-based.

Examples of activities that should be conducted prior to the effective date of registration include:

- ❑ A new Generator Owner should carefully review the applicability section of FAC-003-4 Transmission Vegetation Management
- ❑ Developing programs/procedures where required. For example, PRC-005-6 requires the development of a Protection System Maintenance Program (PSMP).

- ❑ Commissioning equipment and Facilities. While there is not a Reliability Standard that specifically addresses commissioning, it is important that technical rigor is applied during the commissioning process to prevent equipment failures and Misoperations when the Facility is placed in-service. Additionally, the initial due dates for maintenance of Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components under PRC-005-6 are based on the commissioning date of the Components so it is important to retain the commissioning documentation that is used to establish the initial due dates for maintenance activities.
- ❑ Perform initial compliance activities where required. For example, CIP-002-5.1a BES Cyber System Categorization needs to be completed prior to registration, as does the CIP Senior Manager approval of the identified categorizations.
- ❑ Develop processes to meet periodic/time-based and event-driven deadlines for compliance upon NERC registration becoming effective

Upon NERC Registration Becoming Effective

- ❑ Perform, or prepare to perform, event-driven compliance activities (e.g., PRC-004-6, VAR-002-4.1) and retain appropriate evidence.
- ❑ Identify key historical milestone dates (e.g., commissioning, Commercial Operations Date) to establish due dates for initial performance of time-based compliance activities (e.g., MOD-025-2, MOD-026-1, MOD-027-1).
- ❑ Initiate performance of time-based compliance activities and retain appropriate evidence.
- ❑ Follow the guidelines in the NPCC Welcome Letter.
    - Establish account to the NERC Alert System
    - Establish GADS (Generator Availability Data System) account and implement a process for GADS reporting.
    - Establish account to MIDAS (Misoperation Information Data Analysis System) reporting.

ERO Compliance Guidance

Compliance Guidance developed by the ERO under the Compliance Guidance Policy includes two types of guidance documents for registered entities and can be found on the NERC website.

- Implementation Guidance are messages that are developed by industry for registered entity consideration in implementing a Standard.
- CMEP Practice Guides are developed by ERO Enterprise CMEP staff and provide public direction to ERO Enterprise CMEP staff and registered entities on the approaches that CMEP Staff will use to carry out compliance monitoring and enforcement

The Importance of Internal Controls

Internal controls help companies operate effectively and efficiently, reduce the risk of noncompliance, and improve the reliability of the Bulk Electric System (BES). An entity's controls will be assessed as part of the compliance monitoring engagement.

Many entities have internal controls, but sometimes the entities do not always recognize their existing internal controls as "*internal controls.*" Often, this is because the control is part of the company's normal business process and is not specifically called out as an internal control. The discussion below is meant to help entities identify existing internal controls and provide a general overview for building out internal controls for applicable Requirements. More specific considerations are provided in the Internal Controls Considerations section and revolve around the concepts of Preventative, Detective, and Corrective internal controls.

Preventative Controls

Preventative controls aim to reduce the risk of a negative event actually occurring. Preventative controls can be physical or administrative controls depending on the requirement and capabilities at the entity's disposal.

Common administrative preventative controls are automation, procedures, checklists, and training. These tools either prevent the undesirable event from occurring or help personnel understand what things need to be done so that it does not occur.

Detective Controls

Detective controls seek to identify an issue that is occurring or has occurred. For example, the entity could establish alarms to alert operators to an AVR status change and the time that status change occurs. In other words, the alarm detects and alerts personnel to a change from normal operations. A detective control to meet compliance obligations could also be a periodic review of AVR status changes to verify (1) that the appropriate notifications were made and (2) notifications to the TOP(s) meet the time requirement specified in VAR-002-4.1 R3.

Corrective Controls

Corrective controls correct issues once they have occurred and return a situation to its normal state. Using VAR-002-4.1 as the example, a corrective control might include what actions, if any, a generator operator could take to restore the AVR status to normal. Can the generator operator reboot a server? Should the generator operator contact site personnel for assistance? Corrective controls can also be oriented toward re-establishing compliance with a requirement. The entity can, furthermore, determine if additional actions are necessary according to the framework of its Internal Compliance Program (ICP).

Assessing the Effectiveness of Internal Controls

Once an entity has implemented an internal controls framework, the entity should develop internal methods for challenging and testing the controls to verify that they are performing as expected.

Suggested Reading on Internal Controls

ERO Enterprise Guide for Internal Controls

GO/GOP Due Dates for Aspects of Certain Standards

General Procedural			
Standard Requirement	**Function**	**Procedural Requirement**	**Due Date**
EOP-004-4 R1	GO, GOP	Documented Event Report Operating Plan	Registration Effective Date
FAC-003-4 R3	GO	Documented maintenance strategies or procedures or processes or specifications it uses to prevent vegetation encroachments	Registration Effective Date
FAC-008-5 R1, R2	GO	Documentation for determining Facility Ratings and Facility Ratings methodology	Registration Effective Date
PRC-005-6 R1, R2	GO	Documented Protection System Maintenance Program	Registration Effective Date
PRC-027-1 R1	GO	Established process for developing new and revised Protection System settings	Registration Effective Date
Initial Performance			
Standard Requirement	**Function**	**Performance Requirement**	**Due Date**

CIP-002-5.1a R1	GO, GOP	Implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above 1.1 Identify each of the High impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2 Identify each of the Medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3 Identify each asset that contains a Low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	Registration Effective Date
CIP-002-5.1a R2	GO, GOP	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified), even if it has no identified items in Requirement R1 and have its CIP Senior Manager or delegate approve the identifications required by Requirement R1, even if it has no identified items in Requirement R1.	Registration Effective Date
CIP-003-8 R1	GO, GOP	Review and obtain CIP Senior Manager approval for one or more documented cyber security policies that collectively address the topics found in 1.1 (1.1.1 - 1.1.9) and 1.2 (1.2.1-1.2.6).	Registration Effective Date

CIP-003-8 R2	GO, GOP	Implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1 Sections 1-5.	Registration Effective Date
CIP-003-8 R3	GO, GOP	Identify a CIP Senior Manager by name.	Registration Effective Date
CIP-003-8 R4	GO, GOP	Implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	Registration Effective Date
COM-001-3 R8	GOP	Have Interpersonal Communication capability with the BA and TOP	Registration Effective Date
COM-001-3 R12	GOP	Have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES, including includes communication capabilities between Control Centers within the same functional entity, and/or between Control Center and field personnel.	Registration Effective Date
COM-002-4 R3	GOP	Conduct initial training (three-part communication) for each of its operating personnel who can receive an oral two-party, person-to-person Operating Instruction	To meet compliance, training must occur for the individual operator prior to the individual operator receiving an oral two-party, person-

			to-person Operating Instruction However, NPCC highly recommends all individual operators be trained by the Registration Effective Date.
FAC-008-5 R6	GO	Establish Facility Ratings consistent with the Facility Ratings methodology or documentation for determining its Facility Ratings	Registration Effective Date
IRO-010-3 R3	GO	Satisfy obligations of RC data specification	Registration Effective Date
MOD-032-1 R2	GO	Provide steady-state, dynamics, and short circuit modeling data to its Transmission Planner(s) and Planning Coordinator(s) according to the data requirements and reporting procedures developed by its Planning Coordinator and Transmission Planner in Requirement R1	Registration Effective Date
PER-005-2 R6	GOP	Use a systematic approach to develop and implement training to its personnel identified in Applicability Section 4.1.5.1 of this standard, on how their job function(s) impact the reliable operations of the BES during normal and emergency operations	Registration Effective Date
PER-006-1 R1	GOP	Provide training to personnel identified in Applicability section 4.1.1.1. on the operational functionality of Protection Systems and Remedial Action Schemes (RAS) that affect the output of the generating Facility(ies) it operates	Prior to an individual being staffed in a position that is responsible for the Real-time control of a generator and can

			receive Operating Instruction(s)
PRC-019-2 R1	GO	Verify coordination of voltage regulating controls, limit functions, equipment capabilities and Protection System settings.	Registration Effective Date
PRC-024-3 R1, R2	GO	Set frequency and voltage protective relays to not trip for voltage excursion in “no trip zone”	Registration Effective Date
PRC-025-2 R1	GO	Apply settings that are in accordance with PRC-025-2 – Attachment 1	Registration Effective Date
PRC-027-1 R2	GO	Establish Fault current baseline	Registration (if using Option 2 or Option 3)
TOP-003-5 R5	GOP	Satisfy obligations of TOP data specification	Registration Effective Date
VAR-002-4.1 R1	GOP	Operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator	Registration Effective Date
VAR-002-4.1 R2	GOP	Maintain the generator voltage or Reactive Power schedule (within each generating Facility’s capabilities) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator	Registration Effective Date

Time-Based Performance			
Standard Requirement	**Function**	**Performance Requirement**	**Due Date**
FAC-003-4 R6	GO	Perform a Vegetation Inspection of 100% of its applicable transmission lines	Within first calendar year following registration, not to exceed 18 calendar months from registration
FAC-003-4 R7	GO	Complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD	Within first 12 calendar months or by end of first calendar year following registration
MOD-025-2 R1, R2	GO	Provide Transmission Planner with verification of Real and Reactive Power capability	Within 12 calendar months of commercial operation date
MOD-026-1 R2	GO	Provide a verified generator excitation control system or plant volt/var control function model to Transmission Planner	Within 365 calendar days after the commissioning date
MOD-027-1 R2	GO	Provide a verified turbine/governor and load control or active power/frequency control model to Transmission Planner	Within 365 calendar days after the commissioning date
PRC-005-6 R3, R4	GO	Maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components in accordance with Table 1 through Table 5	Four calendar months to 12 calendar years

			following initial commissioning dates
PRC-012-2 R8	GO	Participate in performing a functional test of each of its RAS to verify the overall RAS performance and the proper operation of non-Protection System components	• At least once every six full calendar years for all RAS not designated as limited impact, or • At least once every twelve full calendar years for all RAS designated as limited impact
PRC-027-1 R2	GO	• Option 1: Perform a Protection System Coordination Study; or • Option 2: Compare present Fault current values to an established Fault current baseline and perform a Protection System Coordination Study when the comparison identifies a 15 percent or greater deviation in Fault current values (either three phase or phase to ground) at a bus to which the BES Element is connected, all in a time interval not to exceed six calendar years; or • Option 3: Option 3: Use a combination of the above.	In a time interval not to exceed six calendar years

Internal Controls Considerations for Certain Standards

The table below includes examples and best practices of internal controls for a subset of GO and GOP Standards and Requirements. The existence of mature internal controls are the foundation that will allow for the entity's compliance obligations to remain sustainable over time.

CIP-002-5.1a

Standard Requirement	Control Considerations
CIP-002-5.1a R1 and R2	***Preventative Controls*** ▪ Train personnel on requirements. ▪ Develop a procedure for categorization, review, and approval. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Evaluate all BES assets and Cyber Assets using the impact rating criteria (Attachment 1), BES reliability operating services, and NERC Glossary of Terms. ▪ Document justifications for each identification of BES assets and Cyber Assets. ▪ Inventory all BES assets and Cyber Assets for CIP applicable identifications (BES Cyber Assets, BES Cyber Systems, EACMS, PACS, PCAs). ▪ Ensure the CIP Senior Manager understands and approves the identifications prior to the due date. ▪ Retain all evidence associated with evaluations, justifications, and approvals. ***Detective Controls***

	▪ Reminders for periodic review and update of identifications or accuracy before annual due date. ▪ Utilize a passive or active discovery tool to identify Cyber Assets connected to the network including alerting. ***Corrective Controls*** ▪ Actions required to remediate any late reviews or approvals and update identifications and inventory. ▪ Utilize a tool to quarantine or remove unauthorized Cyber Assets from the network in a timely manner including alerting.

CIP-003-8

Standard Requirement	Control Considerations
CIP-003-8 R1	***Preventative Controls*** ▪ Train personnel on cyber security policies. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Ensure the CIP Senior Manager understands and approves the cyber security policies prior to the due date. ***Detective Controls*** ▪ Reminders for periodic review before annual due date. ***Corrective Controls*** ▪ Actions required to remediate any late reviews or approvals.
CIP-003-8 R2 Section 1	***Preventative Controls*** ▪ Train personnel on cyber security awareness reinforcement. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Utilize multiple methods of reinforcement (direct and indirect communications, etc.). ▪ Retain all evidence associated with reinforcement. ***Detective Controls*** ▪ Reminders for periodic cyber security awareness reinforcement before annual due date. ***Corrective Controls*** ▪ Actions required to remediate any late reinforcements.

CIP-003-8 R2 Section 2	***Preventative Controls*** ▪ Train personnel on physical access controls. ▪ Utilize layered (multiple) physical access controls. ▪ Utilize key management controls for locks, doors, etc. ▪ Utilize a visitor access control program. ▪ Document physical security perimeter diagrams ***Detective Controls*** ▪ Reminders for periodic review of physical access controls. ▪ Utilize alarms and alerting for unauthorized physical access. ***Corrective Controls*** ▪ Actions required to remediate any non-working physical access controls. ▪ Actions required to remediate any unauthorized physical access.
CIP-003-8 R2 Section 3	***Preventative Controls*** ▪ Train personnel on electronic access controls. ▪ Utilize defense in depth electronic access controls applying the concept of least privilege. ▪ Evaluate and document all justifications for inbound and outbound electronic access. ▪ Utilize controls for malicious code and communications. ▪ Utilize controls for vendor remote access. ▪ Document network diagrams ***Detective Controls*** ▪ Reminders for periodic review of electronic access controls. ▪ Utilize alarms and alerting for unauthorized electronic access and malicious code and communications. ***Corrective Controls*** ▪ Actions required to remediate any broadly defined electronic access controls.

	▪ Actions required to remediate any unauthorized electronic access and malicious code and communications.
CIP-003-8 R2 Section 4	***Preventative Controls*** ▪ Train personnel on Cyber Security Incident Response. ▪ Incorporate both the IT and OT personnel including O&P personnel when implementing or testing the Cyber Security Incident response plan(s). ▪ Subscribe to DHS CISA industry alerts. ▪ Retain all evidence associated with testing or actual Reportable Cyber Security Incidents. ***Detective Controls*** ▪ Reminders for periodic testing of the Cyber Security Incident response plan(s). ▪ Utilize security event logs, alarms, and alerting of detected Cyber Security Incidents. ***Corrective Controls*** ▪ Actions required to remediate any late testing. ▪ Actions required to contain, eradicate, or have recovery/incident resolution of Cyber Security Incidents.

CIP-003-8 R2 Section 5	***Preventative Controls*** ▪ Train personnel on Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. ▪ Inventory all TCA and RM including the location where they will be utilized. ▪ Utilize the concept of least privilege and need to know for personnel who need TCA or RM access. ▪ Ensure malicious code detection methods are up to date and effective. ▪ Utilize controls for vendor owned TCA or RM. ▪ Block unauthorized TCA or RM. ▪ Retain all evidence associated with the utilization of any TCA or RM. ***Detective Controls*** ▪ Reminders for periodic review and evaluation of TCA, RM, and malicious code methods. ▪ Utilize security event logs, alarms, and alerting for unauthorized TCA or RM usage. ▪ Utilize security event logs, alarms, and alerting for out of date malicious code methods. ***Corrective Controls*** ▪ Actions required to remediate any unauthorized TCA or RM. ▪ Force malicious code method updates.

CIP-003-8 R3 and R4	***Preventative Controls*** ▪ Train personnel on the identification and documentation of the CIP Senior Manager and delegate(s). ▪ Document the "specific actions" delegate(s) have been granted authority to do, ▪ Retain all evidence associated with CIP Senior Management and delegates identification and changes. ***Detective Controls*** ▪ Reminders for periodic review of the identified CIP Senior Manager and delegates ▪ Reminders to document changes within 30 calendars. ***Corrective Controls*** ▪ Actions required to remediate any undocumented changes within 30 calendar days of a change.

COM-002-4

Standard Requirement	Control Considerations
COM-002-4 General Controls Considerations	***Preventative Controls*** ▪ Training on different types of communication (person-to-person, burst communication, etc.) and definitions. ▪ Develop a method to track training. ***Detective Controls*** ▪ Process to verify the effectiveness of the training. ▪ Process to review and ensure all personnel (within the company or third-party operating personnel) are trained according to the Standard. ***Corrective Controls*** ▪ Provide additional training as necessary based on detective controls.
COM-002-4 R3	▪ Develop onboarding process to identify new operating personnel who require three-part communication training prior to receiving an Operating Instruction. ▪ Develop a process to determine when operating personnel receive their first Operating Instructions to demonstrate that training was conducted prior to receiving an Operating Instruction.

COM-002-4 R6	▪ Process to identify and collect evidence of received Operating Instructions. ▪ Establish a process to review records and verify that operating personnel use three-part communication when receiving Operating Instructions.

MOD-026-1

Standard Requirement	Control Considerations
MOD-026-1 R2	▪ System to track compliance obligation due dates and ensure the verified model is submitted to TP within 365 days after commissioning date and on or before the 10-year anniversary of the last transmittal. ▪ Functional mapping for each applicable generating unit to ensure appropriate entities receive model submissions. ▪ Process to perform internal reviews of work performed by third-party contractors and verify the work and documentation is sufficient to demonstrate compliance with NERC Reliability Standards. ▪ Process to identify changes to the excitation control system or plant volt/var control function that alter the equipment response characteristic and require the GO provide revised model data or plans to perform model verification under MOD-026-1 R4.

PRC-004-6

Standard Requirement	Control Considerations
PRC-004-6 R1	▪ Process to analyze all BES interrupting device operations to determine if the entity's Protection System components caused a Misoperation within 120 days of the BES interrupting device operation. ▪ Training for personnel responsible for analyzing BES interrupting device operations on process to make determination of whether the entity's Protection System components caused a Misoperation. ▪ Automated notification to personnel responsible for analyzing BES interrupting device operations when a BES interrupting device operation occurs. ▪ System to track BES interrupting device operation dates and Misoperation determination dates. ▪ Standardized analysis form with fields to capture information required to demonstrate the entity determined whether its Protection System components caused a Misoperation within 120 days of the BES interrupting device operation. ▪ Management review of analysis forms to verify timeliness, accuracy, and completeness. ▪ Process to submit BES interrupting device operation and Misoperation data to MIDAS and verify MIDAS submission data is consistent with internal data.

PRC-004-6 R5	▪ Process to develop a Corrective Action Plan (CAP) for the identified Protection System component(s), ***and*** perform an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations within 60 calendar days of first identifying a cause of the Misoperation. ▪ Training for responsible personnel on process to develop CAPs and perform evaluation of applicability to the entity's other Protection Systems including other locations. ▪ System to track date cause of Misoperation was identified and date CAP was developed. ▪ Process to track and document evaluation of CAPs applicability to entity's other Protection Systems. ▪ Standardize CAP forms with fields to capture information required to demonstrate development of CAP and evaluation of applicability within 60 calendar days of first identifying a cause of the Misoperation. ▪ Management review of CAP forms to verify timeliness, accuracy, and completeness. ▪ Develop a control to evaluate Standards and requirements that are affected as a result of implementing the CAP, especially if relay setting changes are made.
PRC-004-6 R6	▪ Process to proceed with implementation of CAPs following development and update each CAP if actions or timetables change, until completed. ▪ System to track implementation status of CAPs and timetables for implementation identified in CAPs. ▪ Automated notification when approaching dates associated with timetables for implementation identified in CAPs. ▪ Periodic review of CAP implementation status and timetables identified in CAPs to verify CAPs are on schedule to be implemented within timetables identified in CAP, or if actions or timetables need to be changed.

PRC-005-6

Standard Requirement	Control Considerations
PRC-005-6 R3	▪ Inventory of applicable Protection System Components with mapping of each Component to prescribed maintenance activities. ▪ System to track past maintenance dates and next maintenance due date for each Component. ▪ Automated notification when Components are approaching due date for maintenance activities. ▪ Escalation process when approaching due dates for maintenance activities are not addressed. ▪ System to store maintenance records and ensure maintenance activities recorded have associated maintenance records. ▪ System to store maintenance records and ensure maintenance activities recorded have associated maintenance records. ▪ Process to review maintenance records and ensure records demonstrate performance of prescribed maintenance activities. ▪ Contractual agreements with third-party contractors hired to perform maintenance with specifications to perform prescribed maintenance activities.

PRC-024-2

Standard Requirement	Control Considerations
PRC-024-3 R1, R2	▪ Protection System design process or relay setting philosophy with identification of applicable functions and components (e.g. volts per hertz relays evaluated at nominal frequency, control systems within turbines or inverters that directly trip or provide tripping signals) and specifications to either set protective relays outside of "no trip zone" or document and communicate equipment limitations. *Note: GOs should account for projection of generator voltage protective relay settings to a corresponding POI voltage within the process. PRC-024-2 R2 specifies generator voltage protective relaying shall be set such that it does not trip the generating units as a result of a voltage excursion at the point of interconnection (defined as high voltage side of the generator step-up or collector transformer) that remains within the "no trip zone" of PRC-024 Attachment 2.* ▪ Inventory of all generator protective relays (including protective functions within control systems that directly trip or provide tripping signals to the generator) with identification of frequency and voltage settings on the relays. ▪ Review of relay level one-line diagrams and other design documentation to ensure applicable relays are accounted for within inventory. ▪ Review of settings to verify protective relaying is not set to trip generator in "no trip zone" of Attachment 2, and review of relay setting documentation to verify accurate settings are documented. ▪ Process to identify, document, and communicate equipment limitations to the Planning Coordinator and Transmission Planner. Accurate functional mapping is critical to ensure appropriate entities receive the required communication.

	▪ Change management process for relay setting changes to ensure changes do not cause generators to trip within "no trip zone" of Attachment 1 or Attachment 2.

VAR-002-4.1

Standard Requirement	Control Considerations

VAR-002-4.1 General Controls Considerations	***Preventative Controls*** ▪ Train Generator Operators on developed processes and expectations pertaining to the applicable VAR requirements. ***Detective Controls*** ▪ Establish alarms and perform periodic reviews of events to verify compliance with established processes. ***Corrective Controls*** ▪ Actions required to restore the equipment status to normal.
VAR-002-4.1 R1	▪ Process to verify the generator is in required control mode. ▪ Establish internal controls for detecting AVR status changes and corrective control for restoring AVR to normal operations.
VAR-002-4.1 R2	▪ Process to verify seasonal voltage schedule and to implement any voltage schedule changes. ▪ Evaluate and train personnel on conditions of notification. ▪ Establish detective (e.g., alarms) and corrective internal controls for voltage schedule deviations. ▪ Disseminate and develop process to notify TOP of voltage schedule deviations per conditions of notification.
VAR-002-4.1 R2.1	▪ Develop a strategy to maintain voltage schedule when AVR is out of service. ▪ Consider using a detective control to collect evidence of maintaining the voltage schedule when the AVR is out of service.

VAR-002-4.1 R2.2	▪ Develop a business process for responding to voltage change directives and making notifications when the new schedule cannot be met. ▪ Develop a process to coordinate with the TOP to establish expectations for when a voltage change directive (setpoint change) cannot be met and the TOP requires notification. ▪ Develop internal control for reviewing received voltage change directives and verifying voltage change directive process was followed.
VAR-002-4.1 R2.3	▪ Determine location from which voltage is being monitored and determine if it is at the same location as specified in the voltage schedule. ▪ Implement monitoring at location specified in voltage schedule or develop method for converting voltage values to the point being monitored.
VAR-002-4.1 R3	▪ Develop internal control to identify AVR status changes and time of status change. ▪ Process to notify TOP(s) of AVR status changes and track time of notification. ▪ Develop internal control for identifying and reviewing AVR status changes and verifying the reporting process was followed.
VAR-002-4.1 R4	▪ Identify conditions that could lead to a change in reactive capability and develop methods to identify those conditions when they occur. ▪ Develop process to identify and report to the TOP(s) changes in reactive capability. ▪ Develop internal control for identifying and reviewing changes in reactive power capability and verifying the reporting process was followed.

VAR-002-4.1 R5	▪ Establish process to identify and track requests from the TOP and TP to ensure responses are provided within 30 calendar days of a request. ▪ Process to retain and evaluate evidence for compliance.
VAR-002-4.1 R6	▪ Establish a process to determine if tap settings would violate safety, an equipment rating, or a regulatory or statutory requirement. ▪ Process to document, notify, and provide a technical justification to the TOP if GO cannot meet specifications. ▪ Process to retain and evaluate evidence for compliance.