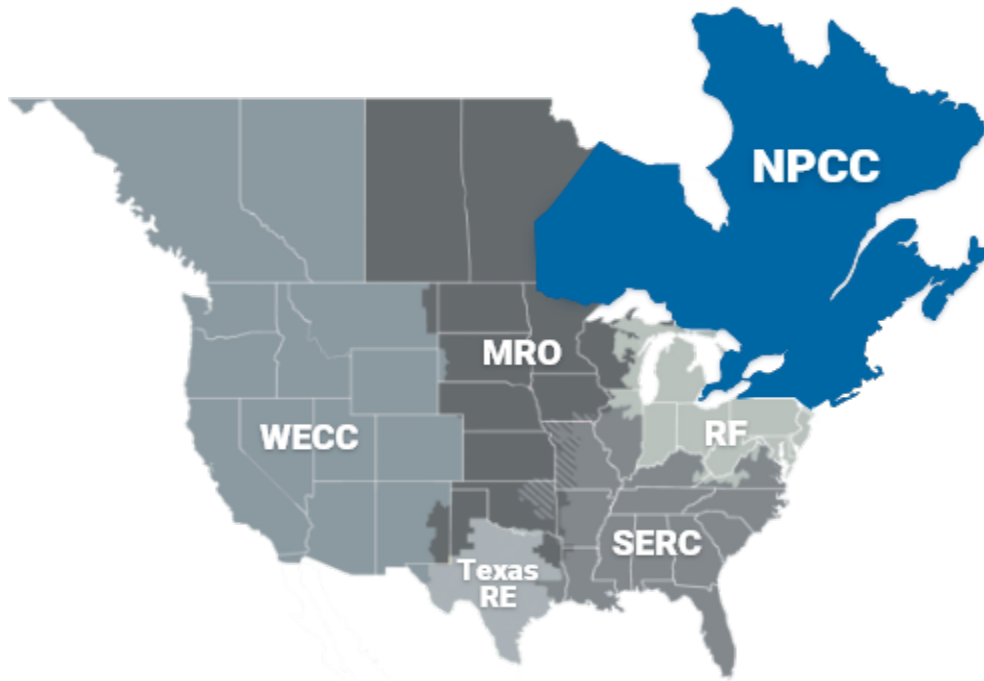


Generator Owner/Operator Welcome Package



July 2026

Table of Contents

Introduction.....	3
Align and Secure Evidence Locker (SEL).....	6
The Importance of Internal Controls.....	7
GO/GOP Due Dates for Aspects of Certain Standards.....	9
Internal Controls Considerations for Certain Standards.....	15
Introduction to NPCC Enforcement.....	25

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 its 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 six to twelve months of preparation before the NERC registration becomes effective, depending on the maturity of the existing compliance program. Entities should ensure they have enough time to develop and implement business processes to meet the applicable Reliability Standards¹. 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 provide high-level timelines, best practices, and recommendations to aid entities in developing a company-specific tracking method.
- 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 does not require a documented procedure explaining three-part communications training. However, entities should consider establishing processes for identifying new operators who

¹ The Standards referenced throughout this Welcome Package are the current active Standards and near-term active Standards when the Welcome Package was posted. NPCC will periodically update the Welcome Package as Standards change.

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. The NERC Consolidated Organization Registration ERO System (CORES), which is accessed via the ERO Portal² is used to submit all registration requests.

NPCC will request a completed ERO Enterprise GO GOP Asset Verification form³. This form contains specific information about the Facility to be registered such as size, interconnection voltage and interconnecting utility.

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 on 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 Transmission Vegetation Management.
- Developing programs/procedures where required. For example, PRC-005 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

² [ERO Portal](#)

³ [ERO Enterprise Generator Asset Verification Form](#)

Relaying Components under PRC-005 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 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, VAR-002) 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, MOD-026).
- Initiate performance of time-based compliance activities and retain appropriate evidence.
- Follow the guidelines in the NPCC Welcome Letter.
 - Establish an account with the NERC Alert System.
 - Establish a GADS (Generator Availability Data System) account and implement a process for GADS reporting.
 - Establish MIDAS (Misoperation Information Data Analysis System) reporting.
- Maintain information in the CORES, such as Primary Compliance Officer, Primary Compliance Contact, Alternate Compliance Contacts, Functional Mapping, etc.
- Become aware of all applicable Periodic Data Submissions required by reviewing the [2026 ERO Periodic Data Submittal Matrix](#).

ERO Compliance Guidance

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

- [Implementation Guidance](#), developed by industry, are documented methods for registered entity consideration during Standard implementation.
- [Compliance Monitoring and Enforcement Program \(CMEP\) 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.

Additional Guidance and Tools

The ERO Enterprise publicly posts additional information to assist registered entities in maintaining and demonstrating compliance. Several important reference materials are provided:

- [ERO Enterprise Entity Onboarding Checklist](#) provides a checklist style list of the tasks expected of a new Registered Entity.
- [CIP Evidence Request Tool \(ERT\) Overview](#) provides guidance on the use and common issues with the ERT.
- [Compliance Monitoring and Enforcement Program \(CMEP\) Resources](#) page of NERC's website contains many additional resources that entities should become familiar with.
- [NPCC 101 – Intro to NPCC and NERC](#) provides valuable historical and background information.
- [NPCC.org](#) provides a variety of reference material regarding Risk, Monitoring, and Enforcement activities which newly Registered Entities should become familiar with.

Align and Secure Evidence Locker (SEL)

Align and the Secure Evidence Locker (SEL) are tools used by NERC, Regional Entities, and registered entities in the conduct of the ERO Enterprise CMEP. Align and the SEL provide:

- A more secure method of managing and storing CMEP data.
- Alignment of common business processes, ensuring consistent practices and data gathering.
- A standardized interface for registered entities to interact with the ERO Enterprise.
- Real-time access to information, eliminating delays and manual communications.
- Consistent application of the CMEP.
- Ease of Access, e.g., ability to download all standards and requirements for use in other systems.

Align Overview

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

SEL Overview

SEL provides enhanced security in evidence collection via a NERC on-premises environment. Moreover, SEL supports effective data and information handling practices.

Additional information and training material about Align and the SEL can be found on the NERC website here: [Align and SEL](#).

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 embedded in the company's normal business processes and is not explicitly identified 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 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 undesirable events 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 R3.

Corrective Controls

Corrective controls correct issues once they have occurred and return a situation to its normal state. Using VAR-002 as an example, 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 and Requirement	Function	Required Procedure	Due Date
EOP-004-4 R1	GO, GOP	Documented Event Report Operating Plan	Registration Effective Date
EOP-012-3 R4	GO	Implement cold weather preparedness plan	Registration Effective Date
FAC-003-5 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 and Requirement	Function	Performance Requirement	Due Date
CIP-002-5.1a R1	GO, GOP	<p>Implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:</p> <ul style="list-style-type: none"> 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 <p>1.1 Identify each of the High impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;</p> <p>1.2 Identify each of the Medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and</p> <p>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).</p>	Registration Effective Date
CIP-002-5.1a R2	GO, GOP	<p>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.</p>	Registration Effective Date
CIP-003-9 R1	GO, GOP	<p>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 (1.2.1-1.2.7).</p>	Registration Effective Date

Initial Performance			
Standard and Requirement	Function	Performance Requirement	Due Date
CIP-003-9 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 1-6.	Registration Effective Date
CIP-003-9 R3	GO, GOP	Identify a CIP Senior Manager by name.	Registration Effective Date
CIP-003-9 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 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

Initial Performance			
Standard and Requirement	Function	Performance Requirement	Due Date
			recommends all individual operators be trained by the Registration Effective Date.
EOP-012-3 R5	GO, GOP	Conduct initial training for maintenance and operations personnel responsible for implementing cold weather preparedness plans.	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-010-4 R3	GO	Satisfy obligations of Reliability Coordinator 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 for 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 excursions in “no trip zone”	Registration Effective Date

Initial Performance			
Standard and Requirement	Function	Performance Requirement	Due 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 Transmission Operator 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 and Requirement	Function	Performance Requirement	Due Date
FAC-003-5 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-003-5 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

Time-Based Performance			
Standard and Requirement	Function	Performance Requirement	Due Date
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-026-2 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
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	<ul style="list-style-type: none"> · 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 a foundation that will allow for the entity’s compliance obligations to remain sustainable over time.

Standard Requirement	Control Considerations
CIP-002-5.1a R1 and R2	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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 identification prior to the due date. ▪ Retain all evidence associated with evaluations, justifications, and approvals. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
CIP-003-9 R1	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic review before annual due date. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any late reviews or approvals.
CIP-003-9 R2 Section 1 “Cyber Security Awareness”	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic cyber security awareness reinforcement before annual due date. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any late reinforcements.
CIP-003-8 R2 Section 2 “Physical Security Controls”	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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 <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic review of physical access controls. ▪ Utilize alarms and alert for unauthorized physical access. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any non-working physical access controls. ▪ Actions required to remediate any unauthorized physical access.
CIP-003-9 R2 Section 3 “Electronic Access Controls”	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Train personnel on electronic access controls. ▪ Utilizing a 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.

Standard Requirement	Control Considerations
	<ul style="list-style-type: none"> ▪ Document network diagrams <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic review of electronic access controls. ▪ Utilize alarms and alerting for unauthorized electronic access and malicious code and communications. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any broadly defined electronic access controls. ▪ Actions required to remediate any unauthorized electronic access and malicious code and communications.
<p>CIP-003-9 R2 Section 4 “Cyber Security Incident Response”</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic testing of the Cyber Security Incident response plan(s). ▪ Utilize security event logs, alarms, and alerts of detected Cyber Security Incidents. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any late testing. ▪ Actions required to contain, eradicate, or have recovery/incident resolution of Cyber Security Incidents.
<p>CIP-003-9 R2 Section 5 “Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation”</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic review and evaluation of TCA, RM, and malicious code methods.

Standard Requirement	Control Considerations
	<ul style="list-style-type: none"> ▪ 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. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any unauthorized TCA or RM. ▪ Force malicious code method updates.
<p>CIP-003-9 R2 Section 6 “Vendor Electronic Remote Access Security Controls”</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Train personnel on vendor remote access procedures, including: <ul style="list-style-type: none"> ○ Which vendors have access ○ When vendors should have access ○ How to grant vendor remote access <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Process for identifying active vendor remote access <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to terminate remote access
<p>CIP-003-9 R3 and R4</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Reminders for periodic review of the identified CIP Senior Manager and delegates ▪ Reminders to document changes within 30 calendar days. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to remediate any undocumented changes within 30 calendar days of a change.
<p>COM-002-4 General Controls Considerations</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Training for different types of communication (person-to-person, burst communication, etc.) and definitions. ▪ Develop a method to track training. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Corrective Controls</p>

Standard Requirement	Control Considerations
	<ul style="list-style-type: none"> ▪ Provide additional training as necessary based on detective controls.
COM-002-4 R3	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Develop onboarding process to identify new operating personnel who require three-part communication training prior to receiving an Operating Instruction. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Develop a method for periodic refresher training.
COM-002-4 R6	<p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Process to identify and collect evidence of Operating Instructions. ▪ Establish a process to review records and verify that operating personnel use three-part communication when receiving Operating Instructions.
MOD-026-2 R2	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
PRC-004-6 R1	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
PRC-004-6 R5	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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 in the process to develop CAPs and perform evaluation of applicability to the entity's other Protection Systems including other locations. ▪ System to track the date the 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. ▪ Develop a control to evaluate Standards and requirements that are affected because of implementing the CAP, especially if relay setting changes are made. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Management review of CAP forms to verify timeliness, accuracy, and completeness.
PRC-004-6 R6	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
<p>PRC-005-6 R3</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ System to track past maintenance dates and next maintenance due dates 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. ▪ Contractual agreements with third-party contractors hired to perform maintenance with specifications to perform prescribed maintenance activities. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Process to review maintenance records and ensure records demonstrate performance of prescribed maintenance activities.
<p>PRC-024-3 R1, R2</p>	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. ▪ Review of relay level one-line diagrams and other design documentation to ensure applicable relays are accounted for within inventory. ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
VAR-002-4.1 General Controls Considerations	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Train Generator Operators on developed processes and expectations pertaining to the applicable VAR requirements. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Establish alarms and perform periodic reviews of events to verify compliance with established processes. <p>Corrective Controls</p> <ul style="list-style-type: none"> ▪ Actions required to restore the equipment status to normal.
VAR-002-4.1 R1	<p>Preventative/Detective Controls</p> <ul style="list-style-type: none"> ▪ 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	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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 processes to notify TOP of voltage schedule deviations per conditions of notification.
VAR-002-4.1 R2.1	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ Develop a strategy to maintain voltage schedule when AVR is out of service.
VAR-002-4.1 R2.2	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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 R3	<p>Preventative/Detective Controls</p> <ul style="list-style-type: none"> ▪ 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.

Standard Requirement	Control Considerations
	<ul style="list-style-type: none"> ▪ Develop internal control for identifying and reviewing AVR status changes and verifying the reporting process was followed.
VAR-002-4.1 R4	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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. <p>Detective Controls</p> <ul style="list-style-type: none"> ▪ Develop internal control for identifying and reviewing changes in reactive power capability and verifying the reporting process was followed.
VAR-002-4.1 R5	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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	<p>Preventative Controls</p> <ul style="list-style-type: none"> ▪ 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.

Introduction to NPCC Enforcement

This section is intended to inform you of NPCC’s enforcement process in the event that you encounter a possible noncompliance.

The objective of the Enforcement review is to determine the extent of the noncompliance, assess the actual and potential risk, and ensure that the noncompliance is corrected and action is taken to prevent recurrence. The Enforcement review is conducted in accordance with the CMEP and applicable NERC Rules of Procedure approved by the applicable regulator (in the United States, the Federal Energy Regulatory Commission). The Potential Noncompliance (PNC) review must have a subject matter expert(s) available for the Enforcement team in case clarification of the submitted data is needed.

NPCC Enforcement Milestones and Deadlines

Please note the important dates/deadlines below (subject to change and may not be inclusive).

Activity	Utilization	Approximate Deadline
Preliminary Screen	To inform you that NPCC has confirmed the Standard and Requirements were applicable, the PNC is not a duplicate of an existing Open Enforcement Action, and to remind you of your obligation to preserve documentation pertaining to the PNC.	Within 10 business days after submittal
Triage	NPCC’s initial risk and mitigation assessment of your submitted PNC to determine priority and level of effort. NPCC internal process only.	Within 14 calendar days after submittal
Request for Information (RFI)	NPCC’s request to your organization to obtain information needed to complete Enforcement review.	Generally, 14 calendar days are given to respond for each RFI.
Request for Settlement	Your request to negotiate the terms of your disposition.	Entities can request settlement at any time.
Compliance Exception (CE)	To inform you that the PNC(s) is being filed as a minimal risk noncompliance with no monetary penalty.	Entity may object to the resolution within 7 calendar days. <ul style="list-style-type: none"> - CE with completed mitigation will be considered closed 60 days

Activity	Utilization	Approximate Deadline
		<p>after submitted to FERC unless NERC or FERC initiate a review within the 60-day review period.</p> <ul style="list-style-type: none"> - A CE with ongoing mitigation will not be closed until the mitigation is complete. <p>Any associated data hold is released 18 months from the date of CE notification or upon completion of mitigation activity, whichever is later.</p>
<p>Find, Fix, Track (FFT)</p>	<p>To inform you that the PNC(s) is being filed as a Minimal/Moderate risk noncompliance with no monetary penalty.</p>	<p>Entity may object to the resolution within 10 calendar days. Entity must provide affidavit within 10 calendar days.</p> <ul style="list-style-type: none"> - FFT with completed mitigation will be considered closed 60 days after FERC submittal unless NERC or FERC initiate a review within the 60-day review period. - FFT with ongoing mitigation will not be closed until the mitigation is complete. <p>Any associated data hold is released 18 months from the date of the FFT treatment Notice or upon completion of mitigation activity, whichever is later.</p>
<p>Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS)</p>	<p>To inform you that the PNC(s) is being considered for a monetary penalty or sanction.</p>	<p>Response required within 30 calendar days following the date of the NAVAPS. Otherwise, entity will have accepted the Compliance Enforcement Authority (CEA)'s determination.</p>

Align – Enforcement Quick Reference Guide

How Do I...?	Video How-to	User Guide or Additional Information
Obtain an ERO Portal Account to access Align		<ul style="list-style-type: none"> - ERO Portal Website - ERO Portal User Setup Guide <ul style="list-style-type: none"> • Creating an ERO Portal Account (Pages 4-27)
Obtain or assign the correct credentials through ERO Portal. Within the ERO Portal, users can request the following access, and the Primary Compliance Contact approves. <ul style="list-style-type: none"> • Align Submitter • Align Reader • Align Editor 		<ul style="list-style-type: none"> - ERO Portal User Setup Guide <ul style="list-style-type: none"> • Requesting Align Access (Pages 28-34) • Approving Align Access Request (Pages 35-37)
Submit a Self-Report or Self-Log	(Video) Creating a Self-Report or Self-Log	<ul style="list-style-type: none"> - (User Guide) Creating a Finding (Pages 8-20)
Submit Mitigation <ul style="list-style-type: none"> • User submits mitigation completion for regional verification 	(Video) Submitting Mitigating Activities	<ul style="list-style-type: none"> - (User Guide) Submitting Mitigating Activities (Pages 28-33) - (User Guide) Submitting Mitigation for CEA Verification (Page 41)
Respond to Noncompliance or Mitigation Requests for Information (RFI)	(Video) Responding to Mitigation RFI	<ul style="list-style-type: none"> - (User Guide) Responding to an RFI (Noncompliance) (Pages 25-28) - (User Guide) Responding to an RFI (Mitigation) (Page 35)

How Do I...?	Video How-to	User Guide or Additional Information
Upload Evidence to the Secure Evidence Locker (SEL) <ul style="list-style-type: none"> • User has SEL Submitter Role • User has access to Align for SEL reference ID User uses a TLS 1.3 compatible browser (e.g.: Chrome and Edge)	(Video) Submitting Evidence to SEL	<ul style="list-style-type: none"> - (Website) SEL Submission Website - (User Guide) SEL
Update Finding with scope expansion.	(Video) Adding Information to a Self-Report after Submitting	<ul style="list-style-type: none"> - (User Guide) Updating a Finding (Pages 21-24)
Submit questions/issues with Align or the SEL *Please add a screenshot of the issue*		<ul style="list-style-type: none"> - NERC Helpdesk Ticketing System