WECC

Generator Welcome Package

WECC Registration

October 16, 2023

Table of Contents

Registration Process Overview

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

The following package provides entities with a framework to prepare a Generator Owner (GO) or Generator Operator (GOP) for their compliance obligations and to internally assess the state of compliance. The package was developed based on experiences with new GOs and GOPs and does not guarantee that compliance will be achieved. However, with proper planning and a framework for assessing compliance, an entity is better prepared to be compliant on its registration date. With this in mind, entities should consider the following points when preparing to bring a new generator online and registering with NERC.

- An entity's compliance obligation begins on the day the entity is registered with NERC unless a Requirement or implementation plan (or other authoritative document) specifies the date the entity must be compliant. **The entity should be audit-ready on the day it is registered with NERC.**
- When bringing a new generator online, compliance considerations must be considered early in the process. Preparing a new GO or GOP for compliance may take 6-12 months of preparation before NERC registration, depending on the maturity of the existing compliance program. Entities should ensure they have sufficient time to develop and implement business processes to address the applicable Reliability Standards[1]. However, much of the evidence gathering and evaluation 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 provide high-level timelines, best practices, and recommendations to aid entities in developing a company-specific tracking method.
- A strong compliance program is generally the result of reliable operations, especially when utilizing operational best practices, and the demonstration of compliance should be the outcome of operational activities.
- Procedures and process documents should define and document the entity's business processes with built-in compliance. **Entities should refrain from writing generic procedures that merely reiterate the Standard language.**
- Although a documented procedure is not always required, entities are encouraged to establish strong operational business processes with preventative, detective, and corrective internal controls for applicable NERC Reliability Standards and Requirements. The business processes

[1] The Reliability Standards referenced throughout this welcome package were active Standards when this document was posted. WECC will periodically update the document as Standards change.

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, and conducting and tracking the training. These processes will be unique to the way the company does business.

- The controls considerations noted in the Internal Controls Considerations tables provide observed best practices and common industry processes and are provided as a guide to help entities when developing internal controls. Similar to designing processes, an entity should develop internal controls appropriate for its organization.

Planning Stages

When bringing a new generator online or establishing a Generator Operator, an entity can think of compliance planning on a continuum, with a key milestone at NERC Registration. There are "pre-registration" compliance activities, such as developing procedures and processes, establishing internal controls, commissioning equipment and Facilities, and performing initial compliance activities where necessary. The end of the pre-registration stage is marked by the completion of NERC Registration. As noted above, the entity's compliance obligation begins on the NERC Registration date. “Post-registration” activities can be either event-driven or time-based, and entities should have processes in place to perform the compliance activities for both types. For example, automatic voltage regulator (AVR) status change notifications are event-driven, and entities are expected to make notifications for AVR status changes starting on the NERC Registration date, while other Standards such as PRC-005-6 and MOD-026-1 are time-based, and entities need to plan to ensure compliance.

Pre-Registration Compliance Example

Review the Interconnection Agreement (IA), which can provide useful information for determining applicability to various Standards and Requirements. The following information can typically be found in the IA:

- Interconnection Tie Line Length (useful for determining FAC-003-4 applicability)
- Location of Point of Interconnection (POI)
- Generator type(s)
- Reactive devices
- MW and MVAR capabilities
- Protection System Component ownership
- TO, TOP, and TP information
- Remedial Action Schemes which the generator may be part of
- Cybersecurity expectations
- Shared Facility expectations

- Requirements for SER, DFR, and/or frequency response.

Review Service Agreements. Examples of possible service agreements are listed below:

- Energy Management/Services Agreements.

Identify the roles and responsibilities based on the review of the services agreement.

- Entity responsible for GO or GOP compliance.
    - The entity that will be registered with NERC and who will be ultimately responsible for the state of compliance.
- Entity responsible for performing the functional obligations for the GO or GOP.
    - If an entity has contracted with another company to perform the functional obligations of the GO or GOP, the NERC registered GO or GOP will be responsible for demonstrating compliance with the NERC Reliability Standards and will likely need to obtain and retain documentation from the contracted entity to demonstrate compliance.

Determine Applicability of NERC Standards, for example:

- PER-005-2 (Note: Whether PER-005 is applicable to the GOP or not, GOPs are encouraged to develop a systematic training program that would include the training required by the NERC Standards)
- PER-006-1
- FAC-003-4
- PRC-012-2 and other RAS-related Requirements.

Note: Entities are encouraged to develop and retain evidence to support determinations that specific Standards/Requirements are not applicable to the entity. This evidence can be gathered from the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), and internal justifications for why the Standard or Requirements do not apply. For example, PRC-002-2 R2 requires the GO to have SER (sequence of event recording) if the GO receives a notification from the TO. If the TO does not notify the GO, the GO should consider reaching out to the TO and request confirmation that SER is not required at the GO's plant. Another example is PER-005-2. If a GOP does not meet the applicability, the GOP should consider developing a justification for the determination of not being applicable and gathering evidence to demonstrate it is not applicable.

Additional pre-registration activities include:

- Writing procedures where required. For example, PRC-005-6 requires a Protection System Maintenance Program (PSMP).
- Commissioning equipment and Facilities. While there is no 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 (see NERC Lessons Learned on Verification of AC Quantities during Protection System Design and Commissioning under "Recommended Reading" below). 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 for compliance activities due following NERC registration (i.e., time-based, and event-driven compliance activities), such as MOD-025-2, PRC-004-6, and VAR-002-4.1.

NERC Registration

NERC Registration is coordinated with the Regional Entity's registration team, and submission of the registration package typically occurs 60 days prior to the planned registration date. Below are common activities that take place during the registration process:

- Review the following: Rules of Procedure Section 500, Organization Registration and Certification, Appendix 5A, Organization Registration and Certification Manual, and Appendix 5B, Statement of Compliance Registry Criteria.
- Submit the NERC registration package to the Regional Entity (more information here).
- Retain NCR Letter for records.
- Additional helpful resources include:
  - ERO Enterprise Registration Procedure
  - ERO Enterprise 101 Informational Package
  - ERO Enterprise Onboarding Checklist
  - ERO Portal User Guide
  - CORES User Guide
  - Align and SEL Training Materials and Information

Post-Registration Compliance Activities

Following NERC registration, entities must be prepared to meet compliance obligations. Some compliance obligations can be planned, but many will be event-driven, such as identification of Protection System Misoperations (PRC-004-6) and notification of AVR status changes (VAR-002-4.1). The list below includes common tasks necessary to maintain and demonstrate compliance with the Reliability Standards and tasks associated with processes developed to support the reliability of the Bulk Electric System (BES).

- Perform, or prepare to perform, event-driven compliance activities (e.g., PRC-004-6, VAR-002-4.1) and retain appropriate evidence.
- Identify key 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).
- Perform initial, time-based compliance activities and retain appropriate evidence.
- Add the newly registered entity to NERC Alerts.
- Register for or add the newly registered entity to MIDAS reporting (a Section 1600 Data Request of the NERC Rules of Procedure and not specifically required for compliance with PRC-004-6), if required.
- Implement a process for GADS reporting, if applicable.

New Entity IRA/COP

WECC aims to perform an Inherent Risk Assessment and provide a Compliance Oversight Plan to newly registered entities within approximately eight months following registration.

Recommended Reading

The following is a list of recommended readings for newly registered entities.

Compliance Guidance

Compliance Guidance developed under the Compliance Guidance Policy includes two types of guidance documents and can be found on the NERC website under Compliance Guidance:

- Implementation Guidance developed by registered entities provides examples for implementing a Standard.
- Compliance Monitoring and Enforcement Program (CMEP) Practice Guides developed by ERO Enterprise CMEP staff provide direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities.
- One-Stop Shop (for CMEP).

NERC Lessons Learned and Event Reports

Below is a brief list of some NERC Lessons Learned and Event Reports relevant to new Facilities and the emerging risks associated with new technologies and the changing resource mix. Registered entities are encouraged to review these reports and evaluate how the recommendations and conclusions may apply to their Facility(ies) and operations. All Lessons Learned are posted here and may provide additional value for entities (e.g., winterization efforts in Lessons Learned 2011). Additionally, all Event Reports are posted here and often provide additional materials that are beneficial to entities (e.g., February 2011 Southwest Cold Weather Event Findings and Recommendations).

NERC Lessons Learned:

- Verification of AC Quantities during Protection System Design and Commissioning
- Substation Fires: Working with First Responders
- Current Drone Usage
- Loss of Wind Turbines due to Transient Voltage Disturbances on the Bulk Transmission System

NERC Event Reports:

- July 2020 San Fernando Solar PV Reduction Disturbance
- April and May 2018 Fault Induced Solar Photovoltaic Resource Interruption Disturbances Report
- October 9, 2017 Canyon 2 Fire Disturbance Report
- August 2016 1200 MW Fault Induced Solar Photovoltaic Resources Interruption Disturbance Report

Additional Resources

The following is a list of resources the GO and GOP can consider participating in and reviewing.

- Regional Entity workshops/training, such as seasonal workshops, Reliability & Security Oversight Monthly Update, etc.
- WECC Committee and Board Meetings
- NERC Committee Meetings
- GridEx and GridSecCon
- Western Interconnection Compliance Forum
- Electricity Information Sharing and Analysis Center

Internal Controls Overview

Internal controls help companies operate effectively and efficiently, reduce the risk of noncompliance, and improve the reliability of the BES. As part of the Compliance Audit, Spot Check, and Self-Certification process, auditors will review subsets of an entity's internal controls. Auditors will then provide feedback to WECC’s Risk Assessment groups for the entity's Compliance Oversight Plan (COP) and to inform future engagements and scopes.

Many entities have internal controls, but 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 internal controls for applicable requirements. More specific considerations are provided in the “Controls Consideration” column of the requirement included in the Internal Controls Considerations tables and revolve around the concepts of Preventative, Detective, and Corrective internal controls. While categorization of controls is not necessary, entities can use this framework when establishing business processes to meet their reliability objectives.

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 requirements and capabilities at the entity's disposal.

Badge readers on a Control Center door is a physical preventative control since it prevents unauthorized physical access into the Control Center. Common administrative preventative controls are procedures, checklists, and training. These tools help personnel understand what needs to be done so a negative event 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 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. In other words, corrective controls return a situation to its normal state. Using a Voltage and Reactive (VAR) Standard as the example, a corrective control might include procedures or technology a Generator Operator could use to restore (i.e., correct) 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 more compliance oriented. If a detective control identifies a potential noncompliance (PNC), the entity can have processes in place that require remediation and filing a Self-Report with its Regional Entity. The entity may also have processes in place to determine if additional actions are necessary according to its Internal Compliance Program (ICP).

Testing Internal Controls

Once an entity has implemented an internal controls framework, it can test the controls to verify that they are performing as expected. In a sense, testing controls is a control *for* the controls.

Suggested Reading

ERO Enterprise Guide for Internal Controls

GO/GOP Roadmap

The table below is split into different sections based on the "type" of requirement. It is intended to help newly registered entities focus efforts on developing expectations for their staff or processes needed to maintain reliability. For example, FAC-003 has a procedural type of requirement and performance requirements listed below. Entities may manage the procedural aspect internally, but the performance requirements may require an outside contractor, which implies contract language, budgeting, and timing considerations to meet the needs.

General Procedural

Standard Requirement	Function	Procedural Requirement	Due 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
EOP-004-4 R1	GO, GOP	Document an Event Report Operating Plan.	Registration Effective Date
EOP-011-2 R7	GO	Implement and maintain one or more cold weather preparedness plan(s) for its generating units.	Registration Effective Date
FAC-003-4 R3	GO	Document maintenance strategies or procedures or processes or specification it uses to prevent vegetation encroachments.	Registration Effective Date
FAC-008-5 R1, R2	GO	Have documentation for determining Facility Ratings and Facility Ratings methodology.	Registration Effective Date
PRC-005-6 R1, R2	GO	Document a Protection System Maintenance Program.	Registration Effective Date
PRC-027-1 R1	GO	Establish a 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 BES; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1. 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 and 1.2	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
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 be compliant, training must occur for the individual operator before the individual operator receiving an oral two-party, person-to-person Operating Instruction. However, WECC highly recommends all individual operators be trained by the Registration Effective Date.
EOP-011-2 R8	GO, GOP	Identify the entity responsible for providing the generating unit-specific training, and provide the training to its maintenance or operations personnel responsible for implementing cold weather preparedness plan(s).	Registration Effective Date
FAC-002-3 R2	GO	Coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator when seeking to interconnect new generation facilities or materially modify existing interconnections of generation facilities.	Registration Effective Date
FAC-002-3 R5	GO	Coordinate and cooperate on studies with its Transmission Planner or Planning Coordinator on	Registration Effective Date

		studies regarding requested interconnections of its facilities.	
FAC-008-5 R6	GO	Establish Facility Ratings consistent with the Facility Ratings methodology or documentation for determining 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 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.	Before an individual is staffed in a position that is responsible for the Real-time control of a generator and can receive Operating Instruction(s).
PRC-002-2 R2	GO	Have SER data for circuit breaker position (open/close) for each circuit breaker it owns connected directly to the BES buses identified in Requirement R1 and associated with the BES Elements at those BES buses.	Registration Effective Date
PRC-002-2 R3	GO	Have FR data to determine the electrical quantities specified in Requirement R3 for each triggered FR for the BES Elements it owns connected to the BES buses identified in Requirement R1.	Registration Effective Date
PRC-002-2 R4	GO	Have FR data as specified in Requirement R3 that meets the criteria specified in Requirement R4.	Registration Effective Date
PRC-002-2 R7	GO	Have DDR data to determine the electrical quantities specified in Requirement R7 for each BES	Registration Effective Date

		Element it owns for which it received notification as identified in Requirement R5.	
PRC-002-2 R8	GO	Have continuous data recording and storage for DDR data for the BES Elements identified in Requirement R5. If the equipment was installed prior to the effective date of this standard and is not capable of continuous recording, triggered records must meet the criteria specified in Requirement R8.	Registration Effective Date
PRC-002-2 R9	GO	Have DDR data that meets the criteria specified in Requirement R9.	Registration Effective Date
PRC-002-2 R10	GO	Time synchronize all SER and FR data for the BES buses identified in Requirement R1 and DDR data for the BES buses identified in Requirement R5 to meet the criteria specified in Requirement R10.	Registration Effective
PRC-012-2 R1	GO	Prior to placing a new or functionally modified RAS in service or retiring an existing RAS, provide the information identified in Attachment 1 for review to the Reliability Coordinator(s) where the RAS is located.	Registration Effective Date
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 the "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)
PRC-027-1 R3	GO	Use its process established in Requirement R1 to develop new and revised Protection System settings for BES Elements.	Registration Effective Date
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 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	Registration Effective Date

		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.	

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 the 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	Four calendar months to 12 calendar

		Components in accordance with Table 1 through Table 5.	years, following initial commissioning dates
PRC-019-2 R1	GO	Coordinate the voltage regulating system controls (including in-service limiters and protection functions) with the applicable equipment capabilities and settings of the applicable Protection System devices and functions.	At a maximum of every five calendar years
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**: Use a combination of the above.	In a time interval not to exceed six calendar years

Internal Controls Considerations Tables

The tables below provide some best practices for some Standards and Requirements. It should not be considered an exhaustive list. Instead, entities can review it as a starting point. A newly registered entity is encouraged to leverage existing organizational controls and establish internal controls tailored to its business processes. These are not Requirements but are provided as a resource to facilitate compliance obligations. In the current risk-based environment, compliance engagements examine whether an entity can demonstrate past compliance, as well as the internal controls an entity has developed and implemented to maintain ongoing compliance. The existence of mature internal controls is the foundation that will allow for the entity's compliance obligations to remain sustainable over time. More detailed Internal Controls guidance for select standards can be found on the WECC website.

CIP-002-5.1a

Standard Requirement	Control Consideration
CIP-002-5.1a R1 and R2	• Train personnel on requirements. • Develop a procedure for categorization, review, and approval. • Establish alerts or reminders to prevent missing due dates, including periodic reviews and updates of identifications for accuracy before the annual due date. • 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 before the due date. • Retain all evidence associated with evaluations, justifications, and approvals. • Utilize a passive or active discovery tool to identify Cyber Assets connected to the network and alert on new assets as discovered. • Establish a process to update identifications and inventory. • Utilize a tool to quarantine or remove unauthorized Cyber Assets from the network promptly and alert on unauthorized assets.

CIP-003-8

Standard Requirement	Control Considerations
CIP-003-8 R1	• Train personnel on cyber security policies. • Establish alerts or reminders to prevent missing due dates, including periodic reviews before the annual due date.

	• Ensure the CIP Senior Manager understands and approves the cyber security policies before the due date.
CIP-003-8 R2 Section 1	• Train personnel on cyber security awareness reinforcement. • Establish alerts or reminders to prevent missing due dates, including periodic cyber security awareness reinforcement before the annual due date. • Utilize multiple methods of reinforcement (direct and indirect communications, etc.). • Retain all evidence associated with reinforcement.
CIP-003-8 R2 Section 2	• 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. • Have a process in place to promptly revoke physical access rights in the case of transfers or terminations. • Establish reminders for periodic review of physical access controls and authorized physical access. • Utilize alarms and alerting for unauthorized physical access. • Establish processes to quickly remediate any non-working physical access controls. • Establish processes to quickly remediate any unauthorized physical access.
CIP-003-8 R2 Section 3	• Train personnel on electronic access controls. • Utilize in-depth defense electronic access controls applying the concept of least privilege. • Evaluate and document all justifications for inbound and outbound electronic access. • Utilize controls for vendor remote access. • Document network diagrams. • Have a process in place to promptly revoke electronic access rights in the case of transfers or terminations. • Establish reminders for periodic review of electronic access controls and authorized electronic access. • Periodically review electronic security logs. • Utilize alarms and alerts for unauthorized electronic access and malicious code and communications. • Establish a process or implement technology solution to quickly remediate any unauthorized electronic access and malicious code and communications.
CIP-003-8 R2 Section 4	• 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. • Establish reminders for periodic testing of Cyber Security Incident response plan(s). • Utilize security event logs, alarms, and alerts to detect Cyber Security Incidents. • Update Cyber Security Incident Response Plan based on lessons learned. • Implement processes to contain, eradicate, or have recovery/incident resolution of Cyber Security Incidents.
CIP-003-8 R2 Section 5	• 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 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. • Logically or physically block the use of unauthorized TCA or RM. • Retain all evidence associated with the utilization of any TCA or RM. • Establish reminders for periodic review and evaluation of TCA, RM, and malicious code methods. • Utilize security event logs, alarms, and alerts for unauthorized TCA or RM usage. • Utilize alerts for out-of-date malicious code methods. • Establish a process to remediate any unauthorized TCA or RM usage. • Implement technical controls to force malicious code method updates.
CIP-003-8 R3 and R4	• 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 delegate identification and changes. • Establish reminders for periodic review of the identified CIP Senior Manager and delegates.

O&P

Standard Requirement	Control Considerations
COM-001-3 R8, R12	• Establish communications procedures or protocols that address the operations of all interpersonal communications equipment. • Establish procedures to address failures of both primary and alternate communications facilities. • Periodically test or review communication equipment to confirm operability.
COM-002-4 General Controls Considerations	• Train on different types of communication (person-to-person, burst communication, etc.) and definitions. • Develop a method to track training. • Establish a process to verify the effectiveness of the training. • Establish a process to review and ensure all personnel (within the company or third-party operating personnel) are trained according to the standard. • Provide additional training as necessary based on detective controls.
COM-002-4 R3	• Develop an onboarding process to identify new operating personnel who require three-part communication training before receiving an Operating Instruction. • Develop a process to determine when operating personnel receive their first Operating Instructions to demonstrate that training was conducted before receiving an Operating Instruction. • For entities with a QSE agreement or a third-party operator, consider a process to periodically verify that all operating personnel at the QSE or third-party operator have received three-part communication training before receiving an Operating Instruction.
COM-002-4 R6	• Establish a process or technology solution 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.
EOP-004-4 R1	• Document organizations that receive event reports, including contact information and specifications. • Provide guidance to SMEs on recognizing and categorizing reportable events. • Establish a review process to ensure applicable reports were filed.
EOP-011-2 R7, R8	• Establish processes to prepare for and mitigate operating emergencies due to cold weather. • Establish processes and train for operating during cold weather emergencies (resiliency plans)

	• Periodically review and update cold weather preparedness plans.
FAC-008 R1, R2, R6	• Establish a record management process to ensure quality Facility Rating data. • Establish a change control process for newly commissioned Facilities, including tracking changes to project plans. • Establish a change control process for changes made in the field, both emergency and planned. • Establish a process to periodically verify equipment in the field. • Identify and record responsibilities between neighboring entities (tie-lines).
MOD-026-1 R2	• Implement a system to track compliance obligation due dates and ensure the verified model is submitted to TP within 365 days after the commissioning date and on or before the 10-year anniversary of the last transmittal. • Map functional relationships for each applicable generating unit to ensure appropriate entities receive model submissions. • Establish a process to perform internal reviews of work performed by third-party contractors and verify the work and documentation are sufficient to demonstrate compliance. • Establish a 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 to provide revised model data or plans to perform model verification under MOD-026-1 R4.
PRC-004-6 R1	• Establish a process to ensure Protection System components are installed and programmed as designed as part of the commissioning process. • Establish a process to analyze all BES interrupting device operations to determine if the entity's Protection System components caused a Misoperation. • Train personnel responsible for analyzing BES interrupting device operations on the process to decide whether the entity's Protection System components caused a Misoperation. • Implement automated notification to personnel responsible for analyzing BES interrupting device operations when a BES interrupting device operation occurs. • Establish a system to track BES interrupting device operation and Misoperation determination dates. • Utilize a standardized format to capture the information required to demonstrate that the entity determined whether its Protection System components caused a Misoperation within 120 days of the BES interrupting device operation. • Establish a review process to verify the timeliness, accuracy, and completeness of the analysis.

	• Implement a 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	• Establish a 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. • Train responsible personnel on a process to develop CAPs and evaluate applicability to the entity's other Protection Systems, including other locations. • Implement a system to track the date the cause of Misoperation was identified and the date the CAP was developed. • Establish a process to track and document the evaluation of the CAP's applicability to the entity's other Protection Systems. • Establish a standardized format to capture the information required to demonstrate the development of CAP and evaluation of applicability within 60 calendar days of first identifying a cause of the Misoperation. • Establish a process to verify the timeliness, accuracy, and completeness of CAPs. • Develop a process 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	• Establish a process to implement CAPs and update each CAP if actions or timetables change, until completed. • Track CAP implementation to identified timetables. • Implement automated notification when approaching dates associated with timetables for implementation identified in CAPs. • Periodically review 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	• Inventory applicable Protection System Components with mapping of each Component to prescribed maintenance activities. • Implement a system to track past maintenance dates and the next maintenance due date for each Component. • Implement automated notification when Components are approaching the due date for maintenance activities. • Establish an escalation process when approaching due dates for maintenance activities still need to be addressed. • Implement a system to store maintenance records and ensure maintenance activities have associated maintenance records.

	• Establish a process to review changes to protection systems before implementation and address impacts when found. • Establish a process to review maintenance records and ensure records demonstrate the performance of prescribed maintenance activities. • Establish a process to track and correct deficiencies discovered during maintenance and testing. • Utilize contractual agreements with third-party contractors to ensure maintenance is performed to entity specifications.
PRC-024-3 R1, R2	• Establish a 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 the projection of generator voltage protective relay settings to a corresponding POI voltage within the process. PRC-024-3 R2 specifies generator voltage protective relaying shall be set such that it does not trip the generating units or cease injecting current as a result of a voltage excursion at the high voltage side of the generator step-up or collector transformer that remains within the "no trip zone" of PRC-024 Attachment 2.* • Inventory 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 relay level one-line diagrams and other design documentation to ensure applicable relays are accounted for within inventory. • Review settings to verify protective relaying is not set to trip generator in "no trip zone" of Attachment 2, and review relay setting documentation to verify accurate settings are documented. • Establish a process to identify, document, and communicate equipment limitations to the Planning Coordinator and Transmission Planner. • Map functional relationships to ensure appropriate entities receive the required communication. • Establish a change management process for relay setting changes to ensure changes do not cause generators to trip within the "no trip zone" of Attachment 1 or Attachment 2
PRC-027-1	• Periodically verify the short-circuit model of the system, including the data used to build the model.

	• Establish processes with specific steps to integrate requirements from other NERC compliance standards, including PRC-019, PRC-024, and PRC-025. • Implement processes and technology to manage relay calculation and setting data. • Establish processes to coordinate protection system settings with electrically joined Facilities, including a method to confirm the other party received updates.
VAR-002-4.1 General Controls Considerations	• Train Generator Operators on developed processes and expectations pertaining to the applicable VAR requirements. • Establish alarms and perform periodic reviews of events to verify compliance with established processes. • Establish processes or technology solutions to restore the equipment status to normal when needed.
VAR -002-4.1 R1	• Establish a process to verify if the generator is in the required control mode. • Establish procedural or technical controls for detecting AVR status changes and corrective control for restoring AVR to normal operations.
VAR-002-4.1 R2	• Establish a process to verify seasonal voltage schedules 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 a process to notify TOP of voltage schedule deviations per conditions of notification.
VAR-002-4.1 R2.1	• Develop a strategy to maintain a voltage schedule when AVR is out of service. • Utilize a technical control to collect evidence of maintaining the voltage schedule when the AVR is out of service.
VAR-002-4.1 R2.2	• Develop a 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. • Establish a process to review received voltage change directives and verify that a voltage change directive process was followed.
VAR-002-4.1 R2.3	• Implement monitoring at the location specified in the voltage schedule or develop a method for converting voltage values to the point being monitored.
VAR-002-4.1 R3	• Develop a process or technical control to identify AVR status changes and the time of status change.

	• Establish a process to notify TOP(s) of AVR status changes and track the time of notification. • Develop a process to identify and review AVR status changes and verify 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 them when they occur. • Develop a process to identify and report to the TOP(s) changes in reactive capability. • Develop a process to identify and review changes in reactive power capability and verify the reporting process was followed.
VAR-002-4.1 R5	• Establish a process to identify and track requests from the TOP and TP to ensure responses are provided within 30 calendar days of a request. • Establish a 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. • Establish a process to document, notify, and provide a technical justification to the TOP if GO cannot meet specifications. • Establish a process to retain and evaluate evidence for compliance.

Disclaimer

WECC receives data used in its analyses from a wide variety of sources. WECC strives to source its data from reliable entities and undertakes reasonable efforts to validate the accuracy of the data used. WECC believes the data contained herein and used in its analyses is accurate and reliable. However, WECC disclaims any and all representations, guarantees, warranties, and liability for the information contained herein and any use thereof. Persons who use and rely on the information contained herein do so at their own risk.

Version History

Modified Date	Modified By	Description
10/16/2023	Sarah Mitchell	Version 1