

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Response to Comments

Project 2021-03 CIP-002

November 2024

RELIABILITY | RESILIENCE | SECURITY



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

Table of Contents

Introduction	iii
Control Center Definition.....	1
Control Center Definition	1
Bulk Electric System (BES) Reference for Transmission Owner	2
Mirror ‘facilities hosting operating personnel’ for Transmission Owner	2
Word Selection.....	3
Structure	4
Utilization of the NERC-Defined Term SCADA	4
Application to HVDC Stations	5
Clarity on use of term “Facilities”	5
Registration Process.....	5
Field Cyber Assets	6
CIP-002-8	7
Incorporating ‘reliability tasks’ in 1.3 for Transmission Operator and/or Transmission Owner	7
Clarity regarding ‘reliability tasks’ language across registered entities	7
Separately identify the physical location of a Control Center from the activities performed	8
Editorial Recommendations for Accuracy/Clarity	8
BES Risk Cannot be Quantified by Counting Lines Operated	9
Applicability of Criterion 2.12 to the Transmission Owner	9
Non-BES Assets in Criterion 2.12.....	10
Criterion 2.12 Table.....	10
Criterion 2.12 Exclusion Clause	10
Implementation Plan.....	11
Perceived Gaps.....	12

Introduction

NERC Project 2021-03 proposes revisions to the Control Center definition and CIP-002-8 Criterion 2.12 in Attachment 1. CIP-002-8 provides “bright-line” criteria for applicable Responsible Entities to categorize their Bulk Electric Systems (BES) Cyber Systems based on the impact to their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the BES. The proposed revisions to Attachment 1 address the categorization of Transmission Owner Control Centers (TOCCs) performing the functional obligations of a Transmission Operator (TOP), specifically those that meet medium impact criteria, and clarify the language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.

There were 63 sets of responses, including comments from approximately 165 different people from approximately 105 companies representing 10 of the industry Segments.

Additional information is available on the [project page](#).

Background

Based on industry feedback, the drafting team (DT) modified the Control Center definition along with CIP-002-8. Please refer to the CIP-002-8 Technical Rationale document for additional justification and information regarding requirements within the proposed standards.

Response to Comments Document Layout

The DT will be responding to all comments in a summary response report. Each chapter covers topics identified throughout the comments received (e.g., Applicability, Definition, Administrative, Requirements, etc.). Comments received are outlined at a high level in each chapter followed by the drafting team’s response on how it considered the comment and the outcome of how the comment was addressed. If you have any questions, please contact standards developer, Dominique Love (Dominique.love@nerc.net).

Thank You

The drafting team thanks industry for your time in reviewing the proposed CIP-002-8 standard and providing comments and proposals for the DT’s consideration. All comments received have been reviewed and discussed. Response to comments have been drafted in a summary response.

Control Center Definition

Control Center Definition

Currently approved definition:

Control Center - One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Draft 1¹ proposed definition:

Control Center - One or more rooms where a responsible entity hosts operating personnel to monitor and control the Bulk Electric System (BES) in real-time, as described below, including any spaces that house the Cyber Assets used by operating personnel to monitor and control the BES in real-time. Cyber Assets used by operating personnel to monitor and control the BES in real-time are generally housed in a centralized location and exclude field assets such as remote terminal units.

1. Operating personnel who perform the Real-time reliability-related tasks of a Reliability Coordinator;
2. Operating personnel who perform the Real-time reliability-related tasks of a Balancing Authority;
3. Operating personnel who perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations;
4. Operating personnel of a Transmission Owner who have the capability to electronically control Transmission Facilities at two or more locations in real-time; or
5. Operating personnel of a Generator Operator who have the capability to electronically control generation Facilities at two or more locations in real-time.

Draft 2² proposed definition:

Control Center - One or more facilities used by the operating personnel described below to monitor and control the Bulk Electric System (BES) in real-time, and any facilities that contain the Cyber Assets required for operating personnel to monitor and control the BES in real-time. Field assets, such as remote terminal units and data aggregators, are excluded from the scope of the Control Center definition.

1. Reliability Coordinator personnel who perform the BES company-specific Real-time reliability-related tasks of a Reliability Coordinator;
2. Balancing Authority personnel who perform the BES company-specific Real-time reliability-related tasks of a Balancing Authority;
3. Transmission Operator personnel who perform the BES company-specific Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations;
4. Transmission Owner personnel who have the capability to control Transmission Facilities at two or more locations using Supervisory control and Data Acquisition (SCADA); or
5. Generator Operator personnel who perform the reliability tasks of a Generator Operator for generation Facilities at two or more locations.

¹ Posted for comment and ballot period September 26 – November 9, 2023

² Posted for comment and ballot period April 2 – May 16, 2024

Draft 3³ proposed definition:

Control Center - One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

OR

One or more facilities of a Transmission Owner that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers and excluding field Cyber Assets used for telemetry.

Bulk Electric System (BES) Reference for Transmission Owner

- Suggest updating to “One or more facilities of a Transmission Owner that have the capability to control the **Bulk Electric System** and to control Transmission Facilities at two or more locations in real-time using SCADA, including their associated data centers, and excluding field Cyber Assets used for telemetry.”
- “One or more facilities of a Transmission Owner that have the capability to control **BES** Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers, and excluding field Cyber Assets used for telemetry.”

DT Response

The concept of BES is already captured in the definition of Facility, defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt capacitor, transformer, etc.). The DT believes that expanding to BES Elements beyond “transmission Facilities”, as contemplated per the proposed language ‘to control the BES and to control Transmission Facilities’, will inappropriately widen the scope and introduce ambiguity. The DT also believes that it is important to retain the term “transmission” to avoid unintended inclusion of other asset types such as distribution or generation assets.

Mirror ‘facilities hosting operating personnel’ for Transmission Owner

- Disagreement with the change from “facilities hosting operating personnel” [for TO] to “facilities having the capability to control transmission Facilities”. The proposed language is inappropriately over-broad and has the potential to errantly identify Transmission Facilities as Control Centers, a function they were never intended to execute. If the TO does not have to have operating personnel hosted in a location (that allows for the control of two or more BES transmission Facilities), are they held to a higher standard than the RC, TOP, and BA entities? The RC, TOP and BA entities are clearly required to be hosting operating personnel according to their applicability in the definition.
- As an example, where an unmanned substation has control of local transmission switching for two different switchyards. Operating personnel are not hosted in the location, but SCADA controls allow for the control of two or more transmission Facilities. The proposed definition identifies this as a Control Room. The fact may be that the two local transmission Facilities are within the same fencing and at the same physical location. Is the intent of the drafting team to define these as control centers?
- Request to exclude ‘regional data concentrators’ by ensuring that the ‘capability to control’ is limited to locations where there is an available operator interface designed for control (not for the ability to configure an interface for control)

³ Posted for comment and ballot period August 29 – October 15, 2024

DT Response

The DT in previous unsuccessful ballots has attempted to clarify the location of the Control Center and its personnel and associated data centers. The industry was clear that it wanted the Control Center definition language for the RC, BA, TOP, and GOP to revert back to the existing Control Center definition, which was done in the recent successful ballot.

The new language in the Control Center definition that specifically applies to the TO is focused on the existence of SCADA (Cyber Assets) that can remotely operate BES Facilities with or without the existence of operating personnel at the Control Center location. The TO's TOP could have access to operate the TO BES Cyber Assets via the TO's SCADA. The important issue is the identification and cyber protection of the TO's SCADA system at the appropriate impact level based on span of control.

A Control Center is a place where, in the normal course of business, management of the BES occurs. Human Machine Interface (HMI) at transmission stations with the capability to monitor and control should not be pulled in. While these systems may be used for local actions, they don't typically have ties back into the larger centralized system. Cyber Assets and HMI at transmission stations with the capability to monitor and control locally should be evaluated based on their location and should have the associated impact level established under CIP-002 Attachment 1.

Early in the project, the DT attempted to define "data concentrators," but could not reach industry consensus. In the Control Center definition, field Cyber Assets, such as some data concentrators or data aggregators, are excluded from the definition. Registered Entities are responsible for reviewing the capabilities of their data concentrators and data aggregators to determine if they are associated with a Control Center or with another type of asset (e.g., station for which it is aggregating data). Data concentrators should then be evaluated based on their location and have the associated impact level established under CIP-002 Attachment 1.

Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

Word Selection

- Change "capability" to "authority", or otherwise strike "capability" from the definition
- Recommendation to replace "facilities" with alternate such as "locations" or sites"
- Concerns raised that a lack of specificity regarding the entity that is responsible to determine what equipment is included in a transmission Facility will lead to inconsistencies in application and enforcement
 - Proposed language: "One or more Transmission Owner facilities, including their associated data centers, and excluding field Cyber Assets used for telemetry, that have the capability in real-time using Supervisory Control and Data Acquisition (SCADA) and host the SCADA, to control multiple transmission Facilities at two or more locations, with the equipment that compromise the transmission Facility being defined by the Transmission Owner."
- Statement that there are specific network architecture scenarios that are not limited to "facilities"
- Replace Cyber Asset with BCS

DT Response

One of the primary objectives of the DT has been to ensure that entities correctly identify Transmission Owner Control Centers (TOCC) and clarify applicability of requirements in CIP-002 such that TOCC are appropriately protected, particularly if the TO has the capability to operate transmission Facilities. The DT recognized during the Field Test that some TOs incorrectly believe that the lack of authority to operate BES Facilities means that they do not have a Control Center. However, entities that lack the authority to operate BES Facilities may still have the capability to do so. The cyber security risk that must be protected is access to the BES Cyber Asset, i.e., the SCADA

system that can control the Facility. For this reason, the DT believes that capability is the correct term to use in the Control Center definition.

The DT explored various alternatives to the lower-case term ‘facilities’ during the drafting process and was unable to agree on a term that appropriately conveyed the variety of configurations that may be present across the industry. After iterating through some more expansive modifications to the Control Center definition, the DT ultimately reverted to the current Control Center definition language as it applies to the RC, BA, TOP, and GOP, including use of the lower-case term ‘facilities’. The current definition includes both lower-case ‘facilities’ and upper-case ‘Facilities’. The DT has received feedback from industry that the distinction between the two terms has been well-established over time and that further clarification is not necessary. With respect to specific network architecture scenarios that are not adequately covered by the existing language, the DT believes that the work needed to resolve these additional challenges that have been raised by the industry extends beyond the scope of the portion of the 2016-02 SAR that was assigned to the 2021-03 DT. Based on industry support for this version of the Control Center definition, the DT has elected not to make any changes.

The DT considered the recommendation to replace ‘Cyber Asset’ with ‘BES Cyber System’ in the language that excludes field Cyber Assets used for telemetry; however, the DT recognizes that Cyber Assets are a subset of BES Cyber Systems and believes that it is more appropriate to be comprehensive in the exclusion.

Structure

- The formatting of the revised Control Center definition is confusing where it uses the term “OR”. Use of all upper-case letters within NERC Standards has generally implied use of an abbreviation.
- Recommend replacing this term with “or” and reformatting the definition to prevent the use of a second paragraph solely to include TO facilities.

DT Response

The revised Control Center definition is intentionally split into two sentences separated by “OR” to logically separate the TOCC from the other Control Center types. The logical interpretation is that one or the other applies. Each entity is responsible for considering both sentences, as appropriate for their registrations, and identifying the appropriate Facilities. The DT is not aware of any acronym “OR” in the NERC Glossary of Terms, or future use of the term/acronym “OR”, that would create confusion.

Utilization of the NERC-Defined Term SCADA

- Recommend to eliminate reference to “SCADA” as it is too prescriptive on technology. SCADA is one method used to operate elements at BES Facilities; however, there are other technologies such as a relay network or other industrialized control system not defined as SCADA [terminal servers, remote management protocols to HMIs, or other similar modern means for remote control].
- Limiting inclusion to only those TO facilities using SCADA protocols for control may introduce a reliability gap where such control is affected using terminal servers, remote management protocols to HMIs, or other similar modern means for remote control. A suggestion may be to review the changes made in CIP-005-6 and CIP-005-7 to describe ‘system-to-system’ relationships between Cyber Assets, which is protocol agnostic and provides some future growth room without requiring standards modification.

DT Response

The term SCADA is defined in the NERC Glossary of Terms as ‘A system of remote control and telemetry used to monitor and control the transmission system’. The DT intentionally used the industry terminology SCADA to avoid technologies in relay networks and access mechanisms. The use of the NERC defined term “SCADA” is intended to exclude Cyber Assets used at a relay maintenance office to change relays setting, which may allow the capability to

remotely operate a breaker. These Cyber Assets would not be considered a Control Center, but may be required to be protected under other cyber security categories. Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

Application to HVDC Stations

- Recommendation to expand exclusion verbiage to include HVDC stations
 - Specific language: “excludes station to station communication for HVDC control functions”
 - One commenter asserts that HVDC systems do not have operational control over other transmission elements.
- Clarification requested to differentiate between local and remote control, with proposal as follows:
 - One or more facilities of a Transmission Owner that have **Cyber Assets with** the capability to **remotely** control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers, and excluding field Cyber Assets used for telemetry **and station to station communication for HVDC control functions**.
- Clarity requested for how HVDC systems are to be considered, specifically when the HVDC local control room only control elements within the HVDC system, including HVDC station to station communication.

DT Response

The station-to-station communication for HVDC control functions may be eligible for exemption under CIP-002-7 Section 4.2.3.3. This version has been filed with FERC and awaiting their approval.

Transmission Owners who have facilities that are capable of controlling High Voltage Direct Current (HVDC) Facilities, each Responsible Entity will need to engage with their Regional Entity in order to determine how the language “transmission Facilities at two or more locations” should be applied based on the specific configuration. The current definition has not changed for Transmission Operators, and thus there is no expected change in applicability to classification of their operated HVDC Facilities. Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

Clarity on use of term “Facilities”

- The definition as proposed is unclear regarding the number of Facilities at another location that must be controlled in order to be considered a Control Center. Suggestion to revise the Control Center definition to be consistent with the examples provided in the Technical Rationale, which clarifies that there must be control of at least two Facilities at another distinct location to be considered a Control Center.

DT Response

When considering the language “transmission Facilities at two or more locations” and “generation Facilities at two or more locations,” it is generally expected that the Facilities will have separate street addresses. Facilities located at a single street address would be associated with a single location. An entity must have more than one Facility and must have Facilities at two or more locations in order to have “transmission Facilities at two or more locations” or “generation Facilities at two or more locations.” The DT believes that the existing examples provided in the technical rationale are adequate and that no language changes are necessary to the Control Center definition.

Registration Process

- The gap that the Control Center definition revision is addressing would be best addressed by NERC in the registration process and not in the modification of the defined term.

- Concern that the expansion of Control Center to Transmission Owners continues to conflict with the role that TO's play in the functional operation of the BES. While there are TOs which function as TOPs, or agents of TOPs, expanding the definition of Control Centers does not really address the problems and risks that these entities represent.

DT Response

The DT feels that it has addressed the gap within the Control Center definition regarding Transmission Owners, as provided for in the scope of the related SAR for this project. The DT has worked to keep the scope of the changes as narrow as possible to avoid creating any unnecessary burden on Transmission Owners. The DT believes that appropriately classifying the Transmission Owner facilities as a Control Center is adequate to address the identified risks to the BES created if those facilities with the capability to control are not adequately protected. These facilities will have the same requirements as a similarly situated Transmission Operator. In addition, the NERC registration process is outside this DT's SAR scope and purview pursuant to the NERC Rules of Procedure.

Field Cyber Assets

- Field Cyber Assets are collectively the 'eyes and ears' of the Control Center for providing the decisional data and wide-area situational awareness, and the broad loss of field telemetry systems has been implicated in causing the inoperability of Control Centers in past NERC Lessons Learned documents. Only considering the impact of singular telemetry devices on the field location they are located at would seem to overly credit the redundancy of having many telemetry devices at the expense of providing CIP protection for any of them, instead of considering them as part of the systems which provide critical data for the Control Center to perform its reliability. If the SDT wishes to address the recently added SAR by suggesting complete removal of these devices from CIP consideration, perhaps an additional field trial or data gathering would provide such support. Even without such global removal language, an entity could provide evidence that the loss, degradation, or misuse such telemetry Cyber Systems do not impact the reliability tasks that they specifically perform if that was the case.

DT Response

In previous unsuccessful ballots, the DT attempted to clarify the electronic remote control of transmission Facilities. In the recent successful ballot, the DT instead used the NERC defined term SCADA, but excluded field Cyber Assets from being considered based on input from industry. The underlying premise is that field Cyber Assets will be evaluated and have the associated impact level established under CIP-002 Attachment 1. Field Cyber Assets will be evaluated along with other asset types (e.g., substation, IROL, etc.) that are subject to CIP-002-8 and would be protected as such. Thus, exclusion from the Control Center definition does not mean that the telemetry goes unprotected. If the field Cyber Assets used for telemetry are incorporated into the Control Center, then the Control Center extends into all of the field Cyber Assets that send information to the Control Center. Thus, everything is high which isn't appropriate from a risk perspective.

Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

Incorporating 'reliability tasks' in 1.3 for Transmission Operator and/or Transmission Owner

- Suggest splitting out part 1.3 in Attachment 1 IRC for TOP and TO, as TOP should have similar wording as per the Control Center definition to the RC, BA, and GOP and the TO should be exclusive to part 1.3 wording.
- Recommended that "reliability tasks" be included in the High Impact Rating Criteria 1.3. for Transmission Operators (TOPs) and Transmission Owners (TOs). The "functional obligations" language in CIP-002-5.1a, Attachment 1, 1.3. for the TOP was removed, but not replaced with "reliability tasks".

DT Response

The DT holds that the distinction between the TO and TOP Control Centers does not carry into the categorization assessment process of Attachment 1 of CIP-002-8. After the TOP or TO has identified a Control Center, the application of part 1.3 has no separate unique application to the TO apart from the TOP registrations. Further, "reliability tasks" have no bearing once the TOP or TO have identified their respective Control Centers as they both have the capability to control transmission Facilities. Inclusion of "reliability tasks" in criterion 1.3 could continue to create confusion over the distinction between the capability to control versus the authority to control. Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

Clarity regarding 'reliability tasks' language across registered entities

- References to "reliability tasks" should align with NERC standard PER-005-2 language and be referred to as "BES company specific Real-time reliability related tasks" to lessen the opportunity for confusion, auditor interpretation, and reliability gaps.
- The language "perform the reliability tasks" is included for the RC, the BA and the GOP. PER-005-2 does not include a requirement for the GOP to "create a list of BES company-specific Real-time reliability-related tasks" (*reliability tasks list*).
- Since 'reliability tasks' is not a defined term, it will be ambiguous without proper expansion within guidelines and technical basis or some other form of guidance.
- It is still not clear in the plain language of the requirement where the 'reliability tasks' of each Responsible Entity are to be derived. To establish a clear linkage for this undefined phrase, perhaps clearly stating that if a task-based responsibility exists in another NERC Reliability Standard, that constitutes a reliability task which bears accounting for in CIP-002-8. Past usage of undefined or non-specific vestigial terminology in CIP-002-5 has led to misunderstanding and inconsistent interpretations.
- The term "reliability tasks" adds no additional clarity. Many transmission owners only manage maintenance, and not operations of their systems. The problem is rooted in the registration where, if an entity does perform TOP reliability tasks, the CEA should force them to be properly registered as a TOP. The Drafting Team has limited ability to address this issue, however, the Drafting Team should recommend that the NERC Functional Model be resurrected and brought up to current industry practices as part of this project.

DT Response

The replacement of 'functional obligations' with 'reliability tasks' was incorporated given that the NERC Functional Model is no longer being actively maintained and to align with the language used in the current Control Center definition. Usage of 'reliability task' is to provide flexibility to an entity when referring to activities performed by that entity to ensure resource adequacy and operational reliability of BES Elements and Facilities. Additional information on the BES reliability operating services that may be useful to entities when they are defining their reliability tasks can be found in the technical rationale document associated with CIP-002-7. Each entity is ultimately responsible for

reviewing their obligations under the NERC Standards to identify their reliability tasks. Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

The DT feels that updating the term “reliability tasks” is outside the scope of the related SAR for this project. The DT does agree that proposed changes to registration classifications and reactivating the NERC Functional Model can be separately discussed with and reviewed by NERC. However, the DT does not feel it is in its purview to make changes.

Separately identify the physical location of a Control Center from the activities performed

- The criteria should be clearer to identify the associated Transmission BES Cyber System and not the physical Control Center. They note that there are many utilities that operate a Transmission and Distribution function out of the same control center. They request that the Drafting Team clearly articulate the difference between Control Center as a place (physical location) and a device (BES Cyber System controlling the BES as per the definition).

DT Response

The changes and language used allow flexibility for entities to define (using the Attachment 1 criteria) the categorization of their specific cyber systems and Cyber Assets, and their associated impact rating. Per the current criteria, an entity defines the impact rating of the BES Cyber System based on its impact to the BES. The flexibility allows entities to develop processes which address the risks posed to the BES by their specific Elements, Facilities, and systems.

In addition, the scope of this DT’s SAR prohibits the expansion of revising the existing standards to address specific BES Control Center functions or technologies beyond the TOCC. The DT does recognize the need to further address technologies and architectures (cloud, virtual Control Centers, AI, etc.) which may patently change the requirements, categorization, and risk posed to an entity and BES at large. A separate SAR would be required to holistically review and revise the Control Center definition to an alternate approach that distinguishes between the physical location of the Control Center and the BES Cyber Systems that provide Control Center functionality.

Editorial Recommendations for Accuracy/Clarity

- A commenter notes the Redline to Last Approved and Redline to Last Posted files have editorial errors in the bullets of Criterion 2.12. The 75 MWh in the second bullet is missing the “h”. Additionally, there should be spaces before the “kV” for “60kV” and “300kV”.
- Another commentor suggests replacing suggests replacing ‘The “aggregate weighted value” for a Control Center or backup Control Center is determined by summing the “weight value per BES Transmission Line” that is monitored and controlled by the Control Center or backup Control Center shown in the table below.’ With ‘The “aggregate weighted value” for a Control Center or backup Control Center is determined by summing the “weight value per BES Transmission Line” shown in the table below, for lines that are monitored and controlled by the Control Center or backup Control Center.’

DT Response

The DT appreciates the diligent red-line review performed and will make the necessary corrections prior to the final posting. Also, the DT has reviewed the recommendation to replace ‘The “aggregate weighted value” for a Control Center or backup Control Center is determined by summing the “weight value per BES Transmission Line” that is monitored and controlled by the Control Center or backup Control Center shown in the table below.’ The “aggregate weighted value” for a Control Center or backup Control Center is determined by summing the “weight value per BES Transmission Line” shown in the table below, for lines that are monitored and controlled by the Control Center or backup Control Center.’ The DT believes this to be a non-substantive change that will help readability while not

changing the scope, applicability, intent of the document, or the actions required by affected entities. This change will be incorporated into the final posting.

BES Risk Cannot be Quantified by Counting Lines Operated

- The risk to the BCS at a Control Center to the reliable operation of the BES is not easily covered by counting the quantity of transmission lines operated. Two Control Centers operating the same number of transmission lines may pose very different risks to the BES. For example, if one Control Center is predominantly operating Transmission lines at substations interconnected with Generation Facilities it may pose more risk than a Control Center operating Transmission lines at substations that are not interconnected with Generation Facilities. They propose the following language for criterion 2.12: Each Control Center or backup Control Center operated by a Transmission Operator or owned by a Transmission Owner.

DT Response

The Field Test has confirmed the existence of TO and TOP small entities' control areas that do not have a significant impact on BES reliability, some of which include interconnected generation. The current enforced language of CIP-002-5.1a is not commensurate with the risk to the BES as applied to smaller entities. The DT has provided updated language that addresses the objectives of the SAR to resolve this issue. Further, Attachment 1 of CIP-002 includes additional criteria that are intended to identify more impactful risks associated with assets, including criterion 2.8 that specifically includes Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission System that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3. Criterion 1.3 appropriately elevates the BES Cyber Systems located at TO and TOP Control Centers for these assets to High Impact.

Applicability of Criterion 2.12 to the Transmission Owner

- A commentor questions why criterion 2.12 is applicable to Transmission Owners rather than just Transmission Operators and notes that "the criterion focuses on the capability of a control center to operate certain BES Facilities, which aligns with the Transmission Operator definition to "operate" transmission Facilities. The Transmission Owner owns and maintains transmission Facilities by definition and does not inherently "operate" them."

DT Response

The DT does not agree with the premise that Transmission Owners do not operate transmission Facilities. The Field Test identified the existence of TOs that have SCADA systems that are used by their personnel to operate transmission Facilities under Operating Instructions from the TOP, or under prior approved protocols to independently operate in emergency conditions. As such, a TO with the capability to control may have a Control Center that needs to be evaluated under criterion 2.12. If a TO does not have a SCADA system and provides Operating Instructions via radio or phone to field personnel to operate transmission Facilities, then the TO does not have a Control Center and is not subject to criterion 2.12 based on the revised Control Center definition.

Non-BES Assets in Criterion 2.12

- Recommendation to add a paragraph or bullet to the Exclusion section of criterion 2.12 to clarify that facilities with an approved BES Exception (or exclusion) for certain facilities may be excluded from the calculation of the aggregate weighted value.
- Transmission lines operated at <100kV are not part of the BES and should not be included in the aggregate weighted value model.

DT Response

The DT recognizes that there is an established process, as documented in Appendix 5C of the NERC Rules of Procedure, that allows entities to request an exception from the application of the NERC definition of Bulk Electric System. An exception may be granted that will have the effect of either including within the BES an Element or Elements that would otherwise be excluded by application of the BES Definition or excluding from the BES an Element or Elements that would otherwise be included by application of the BES Definition.

The table provided in criterion 2.12 specifies that only a “BES Transmission Line” receive a weighted value. Therefore, the DT does not believe that additional language is needed to clarify that non-BES elements may be excluded from the calculation of the aggregate weighted value.

Further, the DT believes that the specific reference to the “BES Transmission Line” in the table makes it adequately clear that it is only a subset of lines below 100kV that are to be considered. Any non-BES Transmission Lines would not be included in the aggregate weighted value calculation. Additional details regarding the inclusion of lines <100kV in the Aggregate Weighted Value calculation can be found in the Technical Rationale.

Criterion 2.12 Table

- There is a gap between the X99 and Y00 “Characteristics of Line” levels. For example, a 199.5kV line is not rated on this table.
- Request explicit explanation in the Standard of the weighted value of zero for “Each BES Transmission Line 500 kV and above.”

DT Response

Regarding the application of the table provided to a line that is nominally rated at 199.5kV, the DT believes this to be more of a theoretical concern than a practical concern. The DT has constructed the table similarly to the corresponding table that applies to Transmission Facilities. The DT is not aware of any significant challenges in interpreting the existing table and believes that deviating from the established structure would create unnecessary confusion.

With respect to the content of the table for BES Transmission Lines 500kV and above, the DT believes that it is appropriate to use “0 (N/A)”. The “(N/A)” has also been added to the corresponding table in criterion 2.5 that applies to Transmission Facilities. No weight is needed for BES Transmission Lines 500kV and above, because criterion 1.3 elevates the BES Cyber Assets used by and located at a Control Center that monitors and controls Transmission Facilities operated at 500kV or higher to high impact.

Criterion 2.12 Exclusion Clause

- Language in the exemption appears to allow for the exclusion of a Control Center if the load in a set of BES Transmission Lines offsets the generation in another set of BES Transmission Lines.

- Use of 75 MWh gross export is problematic and will lead to gaming. There is no precedent for using a MWh value. Instead, the Drafting Team should consider the maximum line rating, since this allows for any situation where power flows may change.
- Request that the Drafting Team provide additional examples of a GCE and what would or would not qualify as a GCE under the proposed 2.12 exclusion criterion.

DT Response

The DT provided flexibility in the language to allow entities to develop processes which include or exclude Elements, Facilities, and/or systems based on their specific risk to the BES. As written, the exclusion language does not allow for exclusion of a Control Center. Rather, an entity may use the exclusion clause to eliminate specifically defined transmission Lines from their recalculated aggregate weighted value, provided they are able to meet and demonstrate adherence to the ‘group of contiguous Elements, (GCE) requirements. Further, the DT has included limits on entities that may pursue an exclusion by limiting those who are eligible to entities with an unadjusted “aggregate weighted value” of less than 12000 and by limiting the gross export of a GCE to 75 MWh. These limits are intended to prevent application of the exclusion to large control areas and to differentiate between non-impactful load serving areas and areas that are more likely to have an impact on the interconnected BES.

Regarding the use of MWh units, as opposed to MW or MVA line capability, the DT originally proposed a 75 MW threshold and determined that it wasn’t an appropriate unit to represent power flow over time. The DT doesn’t believe that an MVA line rating would be appropriate because it doesn’t directly correlate to actual power flow and the resulting impact to the BES if Elements are compromised. Entities will be responsible for providing evidence that they have remained below the 75 MWh threshold to prevent gaming.

Based on industry support for this version of Control Center definition, the DT has elected not to make any changes.

The DT has provided an example GCE in the technical rationale to provide general guidance to the criterion 2.12 Exclusion Clause. Further, criterion 2.12 examples 3 and 4 in the technical rationale include additional detail about how an entity might apply the GCE exclusion. An entity may choose for themselves whether or not to pursue an exclusion under the documented exclusion clause. With respect to an entity’s use of the exclusion clause, it is the entity’s responsibility to determine the most appropriate method to demonstrate their compliance and to retain the evidence necessary.

Implementation Plan

- A commentor expressed concern that if HVDC control functions are considered in scope as a Control Center, additional time would be necessary to meet additional requirements.
- A commentor expressed concern that there is uncertainty in the standard or Implementation Plan on the timeline for an entity who exceeds the 75MWH exclusion threshold to recalculate their CIP-002-8 inclusions. They suggest including a specific example in the Implementation Plan to address this occurrence to reduce ambiguity.
- The 12-month period makes it unclear how new transmission lines are handled even if it is known that they will increase the net export beyond the 75MW threshold. Commentors request clarity on when exceeding the threshold is a planned change, vs an unplanned change and whether an entity could lose the exemption, and then gain it back before the 2-year implementation period is over.
- The proposed 24-month implementation plan has the potential to become very limiting for large entities that could have a large number of new Facilities and facilities due to the current revision of the standard. Recommend additional time of 6-12 months to account for updating tools and models in use for the

current version of the standard and to allow for changes due to standard effectiveness occurring in the middle of a calendar year.

DT Response

Transmission Owners who have facilities that are capable of controlling High Voltage Direct Current (HVDC) Facilities, each Responsible Entity will need to engage with their Regional Entity in order to determine how the language “transmission Facilities at two or more locations” should be applied based on the specific configuration. The current definition has not changed for Transmission Operators, and thus there is no expected change in applicability to classification of their operated HVDC Facilities. Given that the earliest effective date of CIP-002-8 is April 1, 2026 (aligning with the earliest possible effective date of CIP-002-7), the DT believes that entities will have adequate time to evaluate impacts before the 24-month window commences and that no modifications to the Implementation Plan are needed.

Each entity must establish their own process to meet the annual periodicity requirements of CIP-002 and is responsible for setting the periodicity of when they will evaluate for the 75 MWh threshold. The entity must respect their established process, which may prevent the entity from pursuing an exclusion for any transmission Lines per criterion 2.12. The DT does not believe that it is appropriate to create a formal example since it would be subjective and specific to each entity’s process. The criterion 2.12 language and the implementation plan make it clear that the evaluation of the exclusion must be performed annually and coordinated with an entity’s annual CIP-002 review. When considering planned changes, entities should consider the intent of the standard and utilize the exclusion as deemed appropriate. The “Planned or Unplanned Changes” section of the implementation plan governs the amount of time that an entity has to move to the appropriate level of protection.

The DT considered increasing the phased-in implementation date for CIP-002-8, Requirement R1, Attachment 1 criterion 2.12 from 24 months; however, the DT elected to retain a 24-month window as it aligns with the established 24-month window that is currently provided to Responsible Entities who identify their first high impact or medium impact BES Cyber System. The DT does not see the justification for extending the implementation window. Further, given that the earliest effective date of CIP-002-8 is April 1, 2026 (aligning with the earliest possible effective date of CIP-002-7), entities will have adequate time to evaluate impacts before the 24-month window commences.

Perceived Gaps

- A commenter expressed concern with the exemption in 4.2.3.3 and requests rationale on why the drafting team included this exemption.
- Several commenters assert that a gap relating to Transmission Planner and Planning Coordinator identification of IROLs will now materialize as, the Modifications to CIP-002 and CIP-014 portion of Project 2021-03 has not completed prior to the Project 2015-09 revisions went into effect. These commenters request that this project work is not delayed any further.

DT Response

Exemption 4.2.3.3 was added as part of the 2016-02 DT efforts and is part of the NERC Board approved CIP-002-7.

The DT recognizes the concerns related to IROLs and appreciates it being presented. The TOCC portion of Project 2021-03 was assigned as high priority by the Standards Committee (SC). Because of this, and the DT’s recognition that combining both the TOCC and IROL portions together could cause delay in its approval, the DT’s focus was to complete the revisions to the TOCC portion first. Once the TOCC revisions pass final ballot, the DT will then begin to focus its work on the portion of Project 2021-03 addressing the IROL language of CIP-002 and CIP-014.