NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2021-03

CIP-002

Industry Webinar
October 30, 2023

RELIABILITY | RESILIENCE | SECURITY




NERC Antitrust

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

NERC Public Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Webinar Agenda

- Project Background
- Field Test
- Control Center Definition and Technical Rationale
- CIP-002 Criterion 2.12 and Technical Rationale
- Implementation Plan
- Questions & Answers

SDT Members

Name	Entity
Megan Sauter (chair)	Oncor Electric Delivery
Russell A. Noble (vice-chair)	Public Utility District No. 1 of Cowlitz County
Mark R. Atkins	AESI
Brian Evans-Mongeon	Utility Services
Terry Volkmann	Volkmann Consulting
Josh Aldridge	Ferrovial
Josh Powers	SPP
Jennifer Tidwell	Southern Company Service, Inc.

Background

- On May 14, 2020, the NERC Board of Trustees (Board) adopted proposed Reliability Standard CIP-002-6.
  - The proposed Reliability Standard revised Criterion 2.12 to:
    - Clarify the language "used to perform the functional obligation of" in order to recognize the existence of certain Transmission Owner Control Centers (TOCCs) performing Transmission Operator (TOP) reliability functions as medium impact based on an aggregate weighted value of their Transmission Lines.
    - Recognize the existence of registered TOP Control Centers that could be categorized as low impact based on having minimal impact to the Bulk Electric System (BES), if compromised.
- On June 12, 2020, NERC filed with FERC to approve CIP-002-6.

Background

- On February 4, 2021, the NERC Board approved a resolution to withdraw CIP-002-6.
  - NERC asserted that cybersecurity events and evolving threat landscape warranted additional scrutiny to criteria that may permit more entities to categorize BES Cyber Systems as low impact.

Background

- The 2021-03 CIP-002 TOCC Standard Drafting Team (SDT) was formed to conduct further study and recommend next steps, in response to the following language of the 2016-02 SAR.

Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations

V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:

- The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
- The definition of Control Center.
- The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

Background

- The 2021-03 CIP-002 TOCC SDT was tasked by NERC to evaluate the adequacy of Criterion 2.12, with respect to identifying Control Centers used to perform the functional obligations of the TOP, that are not otherwise included in high impact rating, to safeguard reliability.

- In pursuit of this objective, the SDT designed a Field Test to obtain data from TOs and TOPs to validate that the bright line Criterion 2.12 from the withdrawn CIP-002-6 is appropriate and does not expose the Bulk Electric System to vulnerabilities.

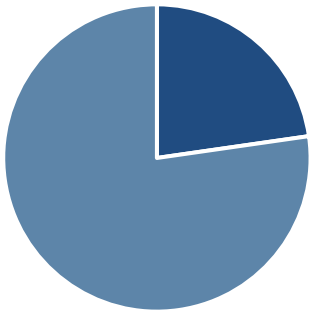
Field Test Questionnaires

- The Field Test was comprised of three questionnaires:
  - Questionnaire 1: The first questionnaire was intended to obtain a range of inherent attributes from each Field Test participants. The results were used to evaluate participant characteristics and to inform the additional information needed from future questionnaires.
  - Questionnaire 2: The second questionnaire requested additional information from participants as necessary to clarify responses from the first questionnaire. Also, participants were asked to perform detailed steady-state power flow studies to simulate specific cyber event scenarios and identify adverse impacts to Bulk Electric System (BES) reliability.
  - Questionnaire 3: The third questionnaire was used to verify aspects of the participant's system and neighboring connections, and also query for characteristics identified by the SDT as indicators of systems that, if compromised, may increase reliability risk to the BES.

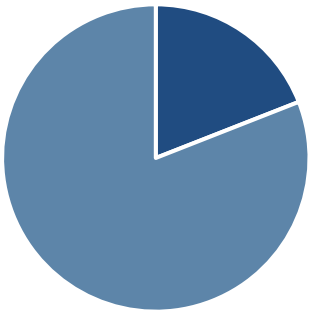
Field Test Participants

- The SDT considered information provided by thirty-seven (37) participants during the Field Test.
- After accounting for participants that withdrew before providing adequate information for full evaluation and participants with systems that were not deemed relevant to the Field Test, a total of twenty-two (22) participants were evaluated by the SDT.

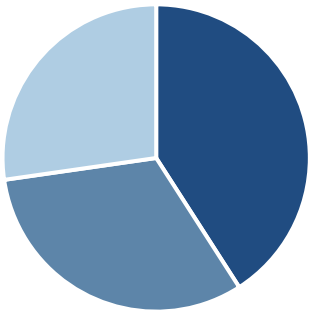
Functional Registration



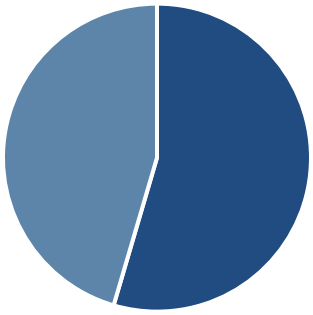
Aggregate Weighted Value



Load Served

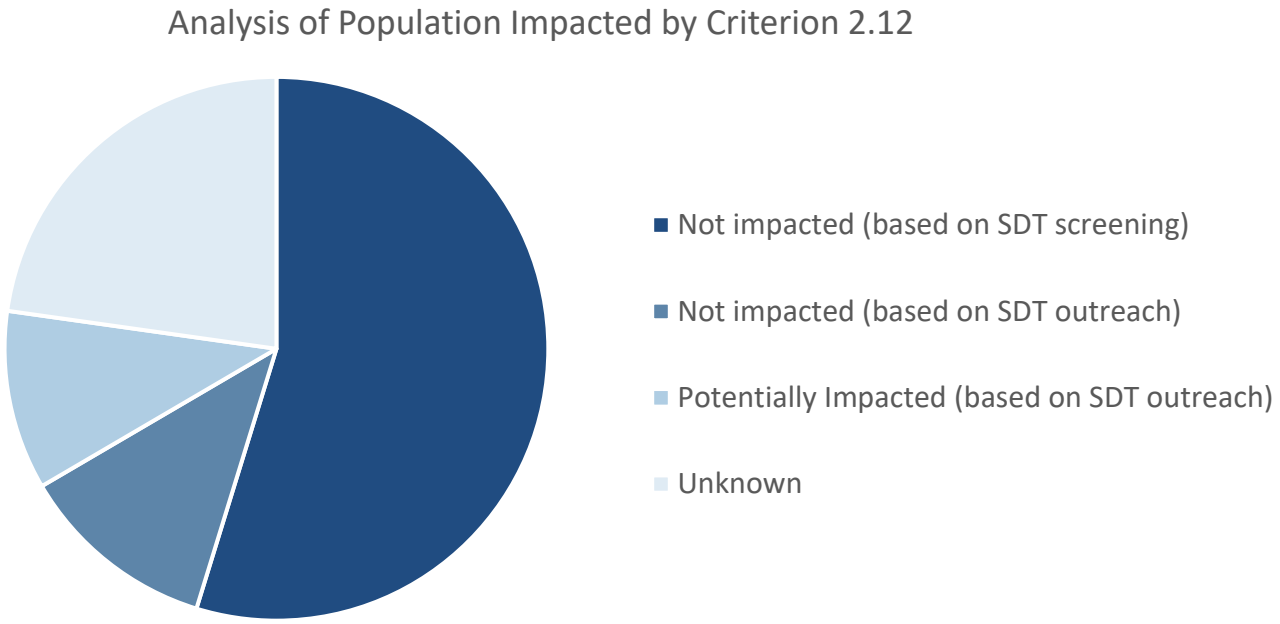


Connected Generation



Field Test Outreach

- The SDT performed an analysis of 347 NERC-registered TOs and TOPs, including direct outreach, to gain a better understanding of the population of entities that could be impacted by a modification to Criterion 2.12.



Field Test Results

- After reviewing all Field Test responses, the SDT has identified that there are entities for which the constraints associated with medium impact rating categorization are not commensurate with the risk posed to the BES should their Control Center be compromised.
  - The SDT did not identify any indicators of adverse impact to the BES for twenty-one (21) of the participants evaluated.
  - One (1) of the participants evaluated by the SDT identified within their system a Transmission Line that is included within the monitored portion of an interface.

Where we are . . .

- An informal comment period was held from June 13 – July 12, 2023 and responses were incorporated in drafting.
- The Quality Review (QR) for this posting was performed from August 18 – August 25, 2023. The QR team included NERC internal staff and experts from the industry.
- At the September 20, 2023 Standard Committee (SC) meeting, the SC authorized initial posting for this project.
  - There are currently two drafting teams working on CIP-002-5.1a. This project is posting modifications as CIP-002-Y to differentiate its work from Project 2016-02 Modifications to CIP Standards (CIP-002-7)

Existing Control Center Definition

- Existing language
  - One or more facilities hosting operating personnel that monitor and control the 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.

Existing Control Center Definition

- While not explicitly listed in the current definition, a TO may have a Control Center through its ability to monitor and control the BES in real-time to perform the reliability tasks of a TOP.

- During the Field Test, the SDT observed that some TOs have struggled to understand application of the existing definition in due to the following:
  - Lack of a common understanding of the term ‘control’ versus ‘authority’
  - Lack of a common understanding of the term ‘perform the functional obligations of the TOP’
  - Lack of a common understanding of the term ‘associated data centers’

Control Center Definition Revisions

Control Center - One or more ~~facilities~~ rooms where a responsible entity hosts ~~hosting~~ operating personnel ~~that~~ to monitor and control the Bulk Electric System (BES) in real-time, as described below, ~~to perform the reliability tasks,~~ 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.~~their associated data centers, of:~~

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 ~~t~~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 ~~for~~ generation Facilities at two or more locations in real-time.

Control Center Definition Rationale

- Use “rooms” in place of “facilities” to eliminate confusion with the defined term “Facility” that is also used in the definition, and to fit a multitude of configurations for different registered entities; focus on where the operating personnel are located.
  - The term “rooms” may include a single room, many rooms within a building, or even an entire building.
  - The term “spaces” was selected with respect to the location of Cyber Assets to recognize that these assets may be housed in a physical or a virtual setting.
- Explicitly identify the five types of registered entities that could have a Control Center to include RC, BA, TOP, TO and GOP.

Control Center Definition Rationale

- Link RC, BA, and TOP operating personnel to the individuals who perform Real-time reliability-related tasks.
- Link TO and GOP operating personnel to those individual having the capability to electronically control Facilities at two or more locations in real-time.
  - The term “capability” is used to clarify that a TOP or GOP that monitors its Facilities without any capability to control those Facilities does not fall within the Control Center definition.
  - The phrase “electronically control” is intended to differentiate between an entity who is able to remotely control BES Facilities in real-time (e.g., via a SCADA system) and an entity who is only able to control BES Facilities via field personnel (e.g., via radio or telephone).
  - Having the capability to electronically control Facilities implies the existence of Cyber Assets to consider under the Cyber Security Standards.

Control Center Definition Rationale

- Eliminate reference to the term “data center” as it has no NERC definition and a wide variety of interpretations.
  - Replace “data centers” with “essential hardware or software used by operating personnel to monitor and control the BES in real-time” to describes the Cyber Assets required for Control Center functions to be performed.
  - Replace “associated” with “spaces that house” to ensure inclusion of locations that contain “essential hardware or software” that may not be located in the same room that hosts operating personnel.
  - Any RTUs or data aggregation assets used to gather and communicate data to the Control Center are specifically excluded. RTUs and data aggregation assets should be evaluated for Cyber Security requirements based on the location and data that they are gathering.

Control Centers in Attachment 1

- Criteria 2.11, 2.12 and 2.13 are unique in the Medium Impact section of Attachment 1, in that they apply to Control Centers.

- As such, additional language was inserted above Criterion 2.11 to replace the language that applies to Criteria 2.1 – 2.10.
  - Language applicable to Criteria 2.1 – 2.10: “Each BES Cyber System, not included in Section 1 above, associated with any of the following”
  - Language applicable to Criteria 2.11 – 2.13: “Each BES Cyber System, not included in Section 1 above, used by and located at any of the following”

Control Centers in Attachment 1

- Technical Rational
  - Language inserted above Criterion 2.11 clarifies the treatment difference between Control Centers and other assets.
    - BES Cyber Systems to consider are those *used by and located at* the Control Center.
    - Intent is to prevent downward expansion into field assets.
    - "Located at" is defined in the Control Center definition and is not limited to a single room, such as where the operating personnel monitor and control the BES in real-time.
    - For other assets such as BES load shedding elements, substations and generation, considered BES Cyber Systems are "associated with" the asset.

Existing Criterion 2.12

- Existing Language
  - Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

- Identified Issues
  - Lacks clarity on applicable functional registrations.
  - Includes entities for which the constraints associated with medium impact rating categorization are not commensurate with the risk posed to the BES should their Control Center be compromised.

Criterion 2.12 Revisions

2.12. Each Control Center or backup Control Center ~~used to perform the functional obligations of the~~, operated by a Transmission Operator or owned by a Transmission Owner, that is not already included in High Impact Rating (H~~),~~) above~~,~~ with an "aggregate weighted value" exceeding 6000 according to the table below and subject to the listed exclusion. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per characteristic" shown in the table for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line
<100 kV	100
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

Exclusion:

BES Transmission Lines monitored and controlled by the Control Center or backup Control Center may be excluded from the "aggregate weighted value" calculation if they are part of a local system that is operated at less than 300kV, where the net export from the local system does not exceed 75 MW during non-Energy Emergency Alert (EEA) conditions. The net export is based on the hourly integrated values for the most recent 12-month period.

Criterion 2.12 Rationale

- Aggregate Weighted Value
  - Intended to measure BES impact by using the total aggregate weighted value of Transmission Lines that are monitored and controlled by a Control Center.
  - Aligns with the methodology used in Criterion 2.5 for the evaluation of Transmission Facilities at stations or substations, by leveraging the nominal operating voltage of BES Transmission Lines, where different voltage values are differently weighted.
  - Weight values for BES Transmission Lines operated at 500kV or above are given a weight value of zero.
    - BES Transmission Lines operated at 500kV or above are subject to Criterion 2.4, whereby the associated Control Centers would be subject to Criterion 1.3.
    - A weight value of zero is assigned to these assets, since Criterion 2.12 would be superseded by Criterion 1.3.

Criterion 2.12 Rationale

- Aggregate Weighted Value (continued)
  - Weight values for BES Transmission Lines operated at 200kV to 499kV follow those established in Criterion 2.5.
  - Weight values for BES Transmission Lines below 200 kV are calculated using MVA values from Appendix A of NERC's Severity Risk Index Enhancements Report, per the process used to establish weight values for BES Transmission Lines operated at 200kV to 499kV.
    - Results were rounded to the nearest 50:
      - 100 – 199kV: (213+160+328)/3 = 233.7, Calculated weighted value = 250
      - Less than 100kV: (64+90+62)/3 = 72, Calculated weighted value = 100
  - BES Transmission Lines less than 100kV are Transmission Lines that have been specifically designated BES via Appendix 5C of the NERC Rules of Procedure.

Criterion 2.12 Rationale

- Aggregate Weighted Value (continued)
  - Total aggregated weighted value bright-line of 6000 is derived from the following:
    - Relevant entities include those that do not have any station or substation meeting Criterion 2.5, whereby the associated Control Center would be subject to Criterion 1.3.
    - Relevant entities are known to monitor and control the BES at two or more locations in real-time per the Control Center definition (i.e., they have a Control Center).
    - The bright-line was established as a proxy for a Control Center with BES Transmission Lines that are equivalent to having two stations or substations meeting Criterion 2.5, in parallel with the “two or more locations” language contained in the Control Center definition.

Criterion 2.12 Rationale

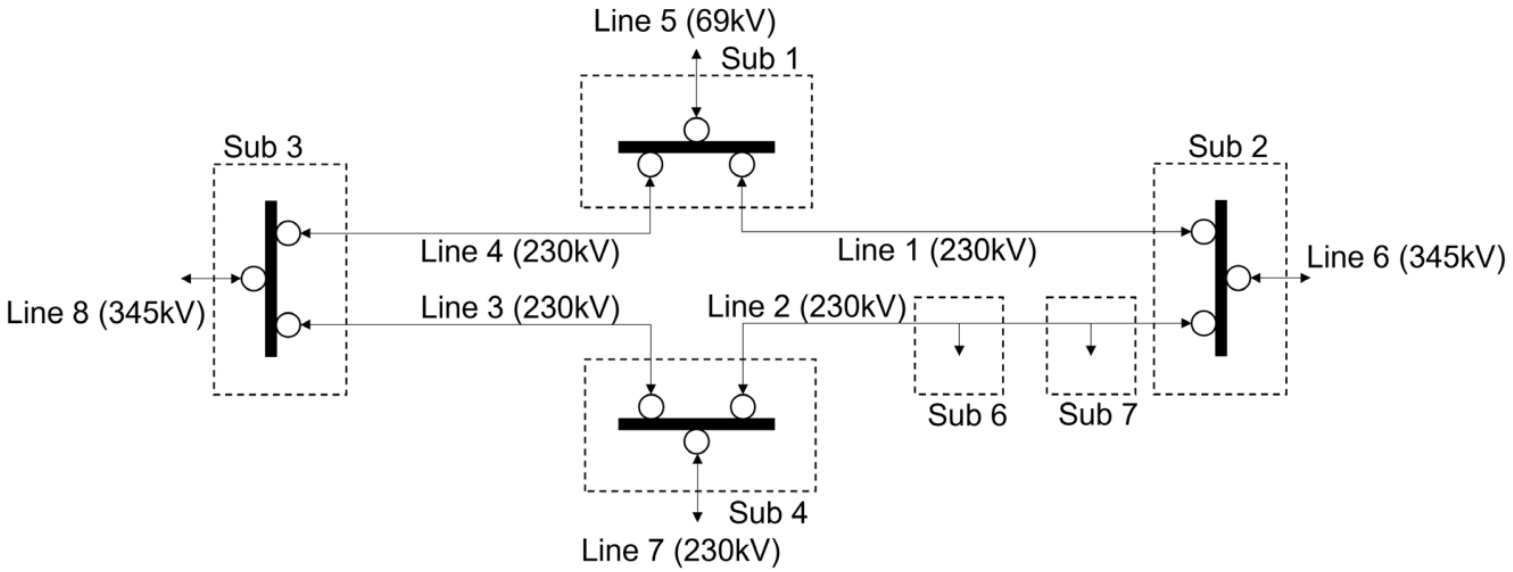
- Exclusion Clause
  - During the Field Test, the SDT observed several participants who exceeded the bright-line of 6000, but did not exhibit any indicators of adverse impact to the BES.
  - Common characteristics of these participants included:
    - Primarily load-serving in nature, with limited or no generation in their area
    - Systems with operating voltages under 300kV
  - An exclusion clause was developed to allow entities meeting the above parameters to exclude BES Transmission Lines serving a local system from the aggregated weighted value calculation if the net export of that local system does not exceed 75 MW.

Criterion 2.12 Rationale

- Exclusion Clause (Continued)
  - The 75 MW net export threshold is aligned with the registration criteria for a Distribution Provider and Generator Owner.
  - The net export is based on the hourly integrated values for the most recent 12-month period.
  - To avoid disincentivizing entities from providing all available assistance during an Energy Emergency Alert, the 75 MW net export limit is excluded in such conditions.

Criterion 2.12 Example 1

- There are two substations shown (Sub 6 and Sub 7) that are tapped on Line 2 for load serving purposes; however, these substations do not have fault interrupting devices that will operate for a fault on Line 2. Therefore, the BES Transmission Line is defined between Sub 2 and Sub 4.
- The entity monitors and controls five (5) 230kV lines and two (2) 345kV lines.



Note: Substation equipment (e.g., transformers) is not shown for simplicity. Circles represent fault interrupting devices.

Criterion 2.12 Example 1

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	Line 1, Line 2, Line 3, Line 4, Line 7	3500
300 kV to 499 kV	1300	Line 6, Line 8	2600
500 kV and above	0	None	0

* Line five is less than 100 kV; however, no exception has been obtained through the NERC Rules of Procedure Exception Process and therefore, the line is not BES.

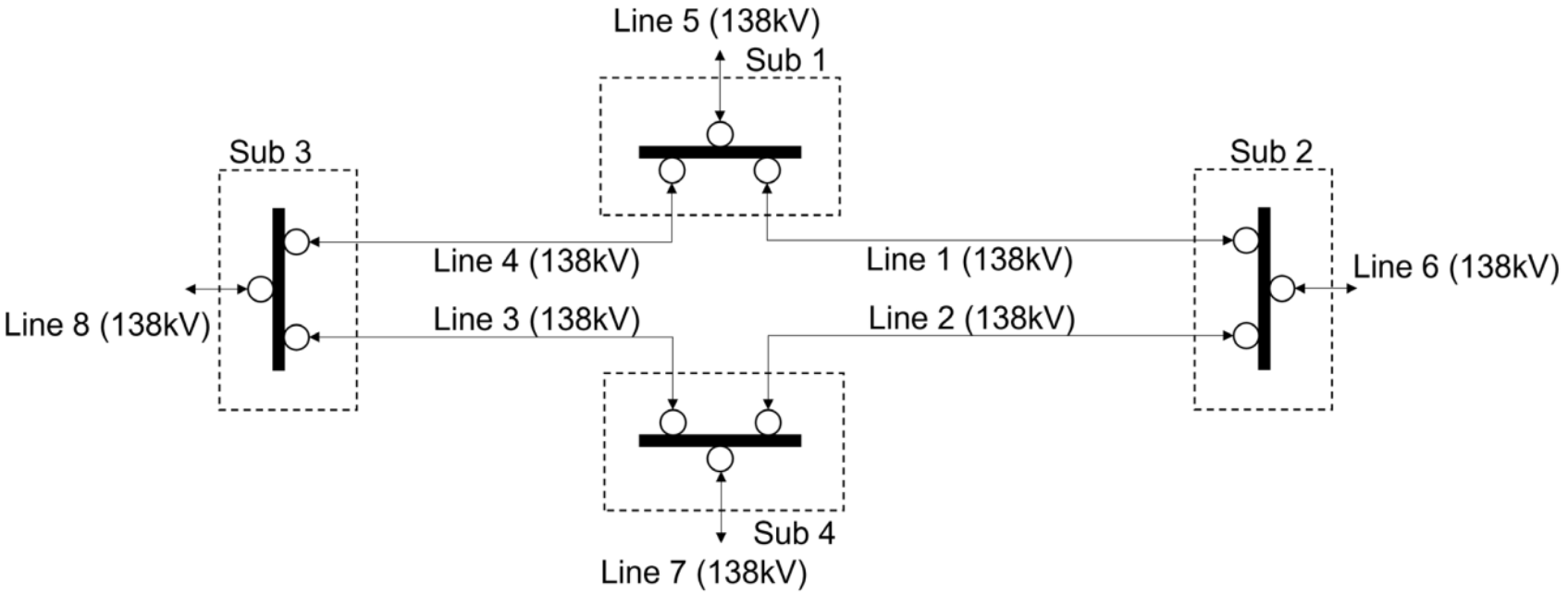
Calculation

700+700+700+700+700+1300+1300 = 6100

- The calculation of the weighted values is demonstrated above and equates to an aggregate weighted value of 6,100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. The BES Cyber System(s) used by and located at the Control Center should be categorized as medium impact BES Cyber System(s).

Criterion 2.12 Example 2

- The entity monitors and controls eight (8) 138kV lines.



Note: Substation equipment (e.g., transformers) is not shown for simplicity. Circles represent fault interrupting devices.

Criterion 2.12 Example 2

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	Line 1, Line 2, Line 3, Line 4, Line 5, Line 6 Line 7, Line 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

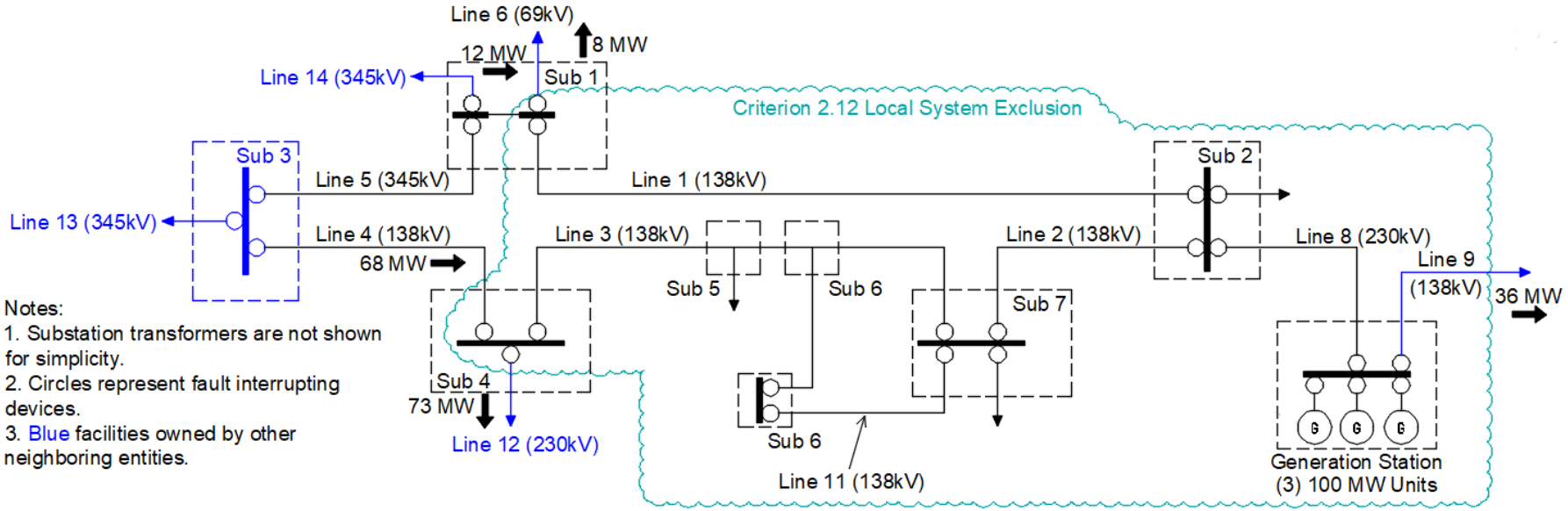
Calculation

250+250+250+250+250+250+250+250 = 2000

- The calculation of the weighted values is demonstrated above and equates to an aggregate weighted value of 2,000, which is below the minimum threshold for the medium impact rating required in Criterion 2.12. The BES Cyber System(s) used by and located at the Control Center should be categorized as low impact BES Cyber System(s).

Criterion 2.12 Example 3

- A local system (not all lines and substations are shown) operating under 300 kV has been excluded as shown below from the aggregate weighted value calculation per the exclusion clause of Criterion 2.12. This is allowed since the maximum hourly integrated value for the last 12-month period (73 – 68 – 12 + 8 + 36 = 37 MW) is less than 75 MW.
- The entity monitors and controls two (2) 345kV lines outside this exclusion area.



Criterion 2.12 Example 3

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	Line 5, Line 14	2600
500 kV and above	0	None	0

Calculation

1300+1300 = 2600

- The calculation of the weighted values is demonstrated above and equates to an aggregate weighted value of 2,600, which is below the minimum threshold for the medium impact rating required in Criterion 2.12. The BES Cyber System(s) used by and located at the Control Center should be categorized as low impact BES Cyber System(s).

Implementation Plan

- Initial Performance of Periodic Requirements in CIP-002-Y
  - Responsible Entities shall initially comply with the periodic requirements in CIP-002-Y, Requirement R2, within 15 calendar months of their last performance of Requirement R2 under CIP-002-5.1a.

- Phased-in Implementation Date for CIP-002-Y, Requirement 1, Attachment 1 Criterion 2.12
  - Provides Responsible Entities a longer implementation period if criterion revisions would result in a higher impact level categorization of a BCS
  - If the changes to Criterion 2.12 result in a higher impact level categorization of a BCS, the Responsible Entity shall not be required to identify that BCS as that higher categorization until **24 calendar months** after the effective date of CIP-002-Y.

Implementation Plan

- Planned or Unplanned Changes
  - The planned and unplanned change provisions in the Implementation Plan associated with CIP-002-5.1a shall apply to CIP-002-Y.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes)	24 months

Next Steps

- Posting
  - Project Page 2021-03
  - 45-day formal comment period from September 26 – November 9, 2023, with ballot pools formed in the first 30 days.
  - Initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period (October 31 – November 9, 2023.)

- Point of Contact
  - Dominique Love, Standards Developer
  - Dominique.Love@nerc.net or call 404-217-7578

Questions and Answers

References

- Project Page 2021-03
- 2016-02 SAR
- Field Test Plan
- Field Test Final Report
- Control Center Definition and CIP-002-Y Red-Line
- Technical Rationale
- CIP version 5 Implementation Plan
- Project 2021-03-CIP-002-Y Implementation Plan
- Unofficial Comment Form