NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 14, 2023

The Honorable Kimberly D. Bose, Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Re: North American Electric Reliability Corporation
Docket No. RD23-2-___

Dear Secretary Bose:

Pursuant to the December 15, 2022 order of the Federal Energy Regulatory Commission in Docket No. RD23-2-000,[1] the North American Electric Reliability Corporation ("NERC") respectfully submits its report on its study evaluating Reliability Standard CIP-014-3. Communications concerning this filing should be directed to:

Shamai Elstein
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005
202-603-3331
shamai.elstein@nerc.net

NERC requests that the Commission accept this report in compliance with the directive in the December 15, 2022 order.

Respectfully submitted,

/s/ Shamai Elstein
Shamai Elstein
Associate General Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005

Counsel for North American Electric Reliability Corporation

[1] *N. Am. Elec. Reliability Corp.*, 181 FERC ¶ 61,230 (2022).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System

April 14, 2023

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

Executive Summary

This report provides the North American Electric Reliability Corporation's ("NERC") updated evaluation of Reliability Standard CIP-014 ("CIP-014" or "Physical Security Reliability Standard"), consistent with the Federal Energy Regulatory Commission's ("FERC" or "Commission") December 15, 2022 order in Docket No. RD23-2-000 (the "December 2022 Order").[1] Due to an increase in reports of physical attacks on electric substations, the Commission issued the December 2022 Order directing NERC to evaluate the effectiveness of the Physical Security Reliability Standard in mitigating the risks to the Bulk-Power System ("BPS") associated with physical attacks.

The Commission directed NERC to evaluate whether the physical security protection requirements in NERC's Reliability Standards are adequate to address the risks associated with physical attacks on BPS Facilities. Specifically, FERC directed NERC to conduct a study evaluating the following: (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard; (2) the adequacy of the required risk assessment set forth in the Physical Security Reliability Standard; and (3) whether a minimum level of physical security protections should be required for all BPS substations and their associated primary control centers.

The purpose of the CIP-014 Reliability Standard is to "identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection."[2] The standard requires applicable Transmission Owners ("TOs") to perform periodic risk assessments of their applicable transmission stations and transmission substations (hereinafter collectively referred to as "substations") to identify which of their applicable substations are "critical" to BPS reliability (which, for purposes of CIP-014, is whether instability, uncontrolled separation, or Cascading would result if the substation were damaged or rendered inoperable). The TO must then perform an evaluation of the potential physical security threats and vulnerabilities of a physical attack to each of their "critical" substations and develop and implement a documented physical security plan to address those threats and vulnerabilities. Additionally, for each primary control center that operationally controls an identified substation, the applicable Transmission Operator ("TOP") must perform an evaluation of the potential physical security threats and vulnerabilities of a physical attack to that control center and develop and implement a documented physical security plan to address those threats and vulnerabilities.

As discussed within this report, NERC finds that the objective of CIP-014 appropriately focuses limited industry resources on risks to the reliable operation of the BPS associated with physical security incidents at the most critical facilities. Based on studies using available data, NERC finds that the CIP-014 Applicability criteria is meeting that objective and is broad enough to capture the subset of applicable facilities that TOs should identify as "critical" pursuant to the risks assessment mandated by Requirement R1. NERC did not find evidence that an expansion of the Applicability criteria would identify additional substations that would qualify as "critical" substations under the CIP-014 Requirement R1 risk assessment. Accordingly, at this time, NERC is not recommending expansion of the CIP-014 Applicability criteria.

NERC acknowledges, however, that supplementary data[3] could show that additional substation configurations would warrant assessment under CIP-014. Accordingly, NERC plans to continue evaluating the adequacy of the Applicability criteria in meeting the objective of CIP-014. Following issuance of this report, NERC will work with FERC staff to hold a technical conference to, among other things, identify the type of substation configurations that should be studied to determine whether any additional substations should be included in the Applicability criteria. The technical conference would also help establish data needs for conducting those studies.

---

1 *N. Am. Elec. Reliability Corp.*, 181 FERC ¶ 61,230 (2022) [hereinafter December 2022 Order].

2 *See* Reliability Standard CIP-014-3 (Physical Security), Section A.3, Purpose. Reliability Standard CIP-014-3 is available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf.

3 Namely, expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration.

NERC finds, however, that the language in Requirement R1 of CIP-014 should be refined to ensure that entities conduct effective risk assessments of their applicable substations. Information from ERO Enterprise Compliance Monitoring and Enforcement Program ("CMEP") activities indicates that while the overall objective of the CIP-014 Requirement R1 risk assessment is sound, there are inconsistent approaches to performing the risk assessment. The ERO Enterprise observed that, in certain instances, registered entities failed to provide sufficient technical studies or justification for study decisions resulting in noncompliance. NERC finds that the inconsistent approach to performing the risk assessment is largely due to a lack of specificity in the requirement language as to the nature and parameters of the risk assessment. Accordingly, NERC will initiate a Reliability Standards development project to evaluate changes to CIP-014 to provide additional clarity on the risk assessment.

As discussed further below, the objective of the Reliability Standards development project would be to:

- Clarify the risk assessment methods for studying instability, uncontrolled separation, and Cascading; such as the expectations of dynamic studies to evaluate for instability.
- Clarify the case(s) used for the assessment to be tailored to the Requirement R1 in-service window and correct any discrepancies between the study period, frequency of study, and the base case a TO uses.
- Clarify the documentation, posting, and usage of known criteria to identify instability, uncontrolled separation, or Cascading as part of the risk assessment. The criteria should also include defining "inoperable" or "damaged" substations such that the intent of the risk assessment is clear.
- Clarify the risk assessment to account for adjacent substations of differing ownership, and substations within line-of-sight to each other.

Finally, while NERC is not recommending an expansion of the CIP-014 Applicability criteria at this time, NERC finds that, given the increase in physical security attacks on BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks associated with those physical security attacks. As discussed further below, establishing a uniform, bright line set of minimum physical security protections for all (or even an additional subset of) BPS substations and associated primary controls centers, is unlikely to be an effective approach to mitigating physical security risks and their potential impacts on the reliable operation of the BPS. While a uniform set of minimum level of protections could potentially prevent some forms of physical security threats, NERC finds that such a pursuit lacks the application of a risk-based approach to expending industry resources, fails to provide for a methodical approach necessary to address site-specific threats or objectives (as expected using a design basis threat process), and does not consider the need for other reliability, resiliency, and security measures to mitigate the impact of a physical attack. These combined measures provide increased operational and planning capability as well as improved effectiveness of local network restoration. NERC finds that this more holistic approach will provide greater long-term flexibility and minimize the impacts of physical attacks on BPS reliability.

To that end, NERC recommends further evaluation of the appropriate combination of reliability, resiliency, and security measures that would be effective in helping to mitigate the impact of physical security attacks. Following issuance of this report, NERC will work with FERC staff to hold a technical conference to gather additional data on these matters and discuss whether and how those measures should be incorporated into NERC's mandatory Reliability Standards. NERC will consult with FERC in the development of the technical conference to discuss, among other things, the following topics:

- The appropriate risk-based approach to identifying the objective of any minimum level of protections, risks to be mitigated, and industry resources necessary to meet such minimum requirements.
- Expanding the use of planning studies, conducted by Transmission Planners ("TPs") under Reliability Standard TPL-001 to evaluate physical security attacks, identify applicable study criteria, and contain a corrective action plan to mitigate inadequate performance against such criteria.

- Enhancing Operational Planning Assessments to include loss of assets (transmission or generation) from physical attacks.
- Enhancing TP and TO requirements to ensure spare equipment pool strategies are adaptive, in-sync, and provide sufficient wide area coverage.
- Requiring Reliability Coordinators ("RCs") to develop and train to readiness scenarios reflecting a physical security incident with TOs, TOPs, Generator Owners, and Generator Operators.

NERC will use the information learned during the technical conference described above to determine the next steps, including potential Reliability Standards modifications.

NERC will also continue its significant efforts outside the context of mandatory Reliability Standards to mitigate the potential for and impact of physical security attacks across the grid. NERC, through the E-ISAC and other mechanisms, has worked extensively with industry to raise awareness of physical security threats and vulnerabilities and develop tools and guidance to promote and facilitate enhanced physical security protection and response measures across the industry. The E-ISAC established the Physical Security Advisory Group, which is an E-ISAC-led group comprised of industry participants that provides expertise to advise industry on threat mitigation strategies to enhance the BPS's physical security and reliability. The E-ISAC regularly holds Vulnerability of Integrated Security Analysis ("VISA") workshops at utility facilities to demonstrate how to implement the VISA process. The VISA process is a scenario-based, vulnerability assessment tool to analyze the effectiveness of security measures to prevent, detect, delay, and respond to attacks. The E-ISAC has also recently released materials to aid and assist entities to better prepare their assets against malicious physical attacks. These materials include the *Physical Security Resource Guide for Electricity Asset Owners and Operators*, which is available on the E-ISAC portal.[4]

[4] Available at: https://eisac-portal.force.com/eisacportal/s/article/E-ISAC-Physical-Security-Resource-Guide-January-2023.

Background

CIP-014 Development and History

NERC initially developed the CIP-014 Reliability Standard in response to a Commission order issued March 7, 2014 in Docket No. RD14-6-000 directing NERC to submit for approval one or more Reliability Standards to address physical security risks and vulnerabilities to critical BPS substations and control centers.[5] In the March 2014 Order, the Commission determined that physical attacks on the BPS could adversely impact reliable operation of the BPS, resulting in instability, uncontrolled separation, or Cascading failures. The Commission noted that the then current Reliability Standards did not specifically require registered entities to take steps to protect against physical security attacks on the BPS. Accordingly, the Commission directed NERC to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of BPS "critical facilities."

The March 2014 Order indicated that the Reliability Standards should require owners or operators of the BPS to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the BPS: (1) owners or operators of the BPS should perform a risk assessment of their systems to identify their "critical facilities"; (2) owners or operators of the identified "critical facilities" should evaluate the potential threats and vulnerabilities to those identified "critical facilities"; and (3) those owners or operators of "critical facilities" should develop and implement a security plan designed to protect against attacks to those identified "critical facilities" based on the assessment of the potential threats and vulnerabilities to their physical security. In the March 2014 Order, the Commission stated that a "critical facility" is "one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[6]

On May 23, 2014, NERC petitioned the Commission to approve Reliability Standard CIP-014-1. NERC explained that Reliability Standard CIP-014-1 "serves the vital reliability goal of enhancing physical security measures for the most critical [BPS] facilities and lessening the overall vulnerability of the [BPS] to physical attacks."[7] NERC stated that the "appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the [BPS]."[8] As noted above, consistent with the March 2014 Order, the purpose of the CIP-014 Reliability Standard is "identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an interconnection." The Commission approved CIP-014-1 on November 20, 2014 in Order No. 802, finding that the standard satisfied the directives in the March 2014 Order.[9]

The CIP-014 Applicability criteria match the "Medium Impact" criteria for transmission facilities listed in Attachment 1 of Reliability Standard CIP-002-5.1a. The Facilities include:

1. Transmission facilities operated at 500 kV or higher;
2. Transmission facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and that exceeds an "aggregated weighted value" as defined in the standard;

---

5 Reliability Standards for Physical Security Measures, 146 FERC ¶ 61,166 (2014) [hereinafter March 2014 Order].

6 *Id.* at P 6.

7 NERC, *Petition of NERC for Approval of Proposed Reliability Standard CIP-014-1*, Docket No. RD14-6-000 at 15-16 (Mar. 7, 2014).

8 *Id.* at 18.

9 *Physical Security Reliability Standard*, Order No. 802, 149 FERC ¶ 61,140 (2014). Since the issuance of Order No. 802 the Commission approved minor modifications to the CIP-014 standard to remove the term "widespread" to Requirement R1 and to remove the provision from the Compliance section that required all evidence demonstrating compliance with the standard to be retained at the Transmission Owner's or Transmission Operator's facility.

3. Transmission facilities at a single station or substation location that are identified by its Reliability Coordinator ("RC"), Planning Coordinator ("PC"), or Transmission Planner ("TP") as critical to the derivation of Interconnection Reliability Operating Limits and their associated contingencies; and
4. Transmission Facilities identified as essential to meeting nuclear plant interface requirements.

The CIP-014-1 Standard Drafting Team adopted these Applicability criteria as the Commission had previously approved them as a technically sound basis for identifying Transmission Facilities, which, if compromised, would present an elevated risk to the BPS.

FERC Order Directing Study of CIP-014

On December 15, 2022, the Commission directed NERC

> to conduct a study evaluating (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard CIP-014-3 (Physical Security Reliability Standard); (2) the required risk assessment set forth in the Physical Security Reliability Standard; and (3) whether a minimum level of physical security protections should be required for all Bulk-Power System transmission stations and substations and primary control centers.[10]

The Commission directed that NERC submit a report to the Commission on the study's findings and recommendations within 120 days of the date of the order.[11]

The Commission explained that it was directing this evaluation because "there has been an increase in reports of physical attacks on electric substations" in recent months, some of which resulted in customer outages.[12] In particular, the Commission cited the December 3, 2022 physical attacks on substations in Moore County, North Carolina, the November 2022 incidents at several Pacific Northwest substations, and that Federal authorities disrupted recent planned attacks before they were perpetrated.

10 December 2022 Order at P 1.
11 *Id*.
12 *Id.* at P 6.

Data Inputs

This section describes the scope of the data reviewed, sources of CIP-014 subject matter expertise, and more general physical security experts consulted to conduct this evaluation and substantiate the report findings. As discussed below, to conduct this evaluation, NERC gathered data from various ERO Enterprise groups and planning cases. Further, NERC identified substation kV class and adjacency using the transmission models representing the Facilities of the Bulk Electric System, and used that data as part of this evaluation.

Regional Entity Subject Matter Experts

Regional Entity subject matter experts ("SMEs") provided their perspectives, data, and insights throughout the assessment. These SMEs reviewed the content of this report for clarity, the completeness of the conclusions, and the engineering judgement used to support the recommendations. NERC will continue to engage Regional Entity SMEs for ongoing physical security threat activities.

Electric Information Sharing and Analysis Center

Finally, NERC consulted the Electric Information Sharing and Analysis Center ("E-ISAC") for data on recent physical security attacks, the nature of physical security threats and vulnerabilities, and best practices for implementing physical security protections. In particular, this consultation leveraged E-ISAC BPS physical security threat experience and awareness to support the findings within the section of this report pertaining to an evaluation of "minimum level of physical security" at all BPS substations and associated primary control centers.

Review of Planning Case Data

This report uses the topology of Interconnection-wide base cases to estimate the number of BPS substations in the Interconnection. Those estimates are based on the following criteria:

- The high side and low side of a transformer are located in the same substation;
- If it exists, the terminals of a circuit breaker are located in the same substation;
- The terminals of series capacitors are in the same substation;
- The terminals of multi-section lines are in different substations (e.g., tapping of a line); and
- A substation has a significant impedance between its neighboring substations.

The topology estimates assumed that a substation impedance[13] would have a greater than 0.2km distance. A high-end estimate (signifying a lower count of estimated substations) increases this distance to 1 km. Using these criteria, the maximum amount of substations found in each interconnection are found in **Table 1**. Also included are estimations from Form EIA-860 data in a separate row and the estimations of the topology including only Bulk Electric System substations found.[14] Differences in the EIA data forms and the planning model representing a substation account for the numerical differences between the models. The primary difference is that the planning model estimates may count multiple generator unit buses (if modeled explicitly) feeding the primary substation and switchyard to the plant. With the EIA data this is counted as one substation, while the planning model may count this as multiple due to isolating on impedance. The topology estimate of the planning model, however, can readily provide connected substations, ratings of the lines connecting the substations, and the lines' nominal kV.

[13] Impedances in the Interconnection-wide base cases are typically in per unit (p.u.), meaning they are a function of the system base MVA and their nominal kV. This check for distance converts the p.u. of the line into a regular impedance (in Ohms) and uses an assumed impedance per mile when comparing to this distance threshold.

[14] The U.S. Energy Information Administration's Form EIA-860 collects generator-level specific information about existing and planned generators and associated environmental equipment at electric power plants with 1 megawatt or greater of combined nameplate capacity.

Table 1: Estimation of Substations

Source	EI	TI	WI
Topology Estimate	56,767	5,236	11,948
Topology Estimate (only BES)	25,000+	3,662	7,854
Energy Information Agency (U.S. Only)	40,608	2,546	10,992
Energy Information Agency (BES U.S. Only)	39,000	3,500	10,000

The information in **Table 1** can be graphically compared to **Figure 1** which uses the planning case estimates and **Figure 2** which uses the EIA data sources. Comparing the ratios currently applicable to CIP-014-3 (>345 kV, >200 kV, >100 kV) and all other buses in the data source indicates that both data sets contain roughly the same percentage of substations. Again, this indicates that the topology estimation using the planning case data is a representative sample of all substations in each Interconnection, and that the percentage composition of these substations is generally aligned. Based on these comparisons and the benefit of other data fields of the planning model, the team favors analysis using the planning model numbers for assessing the adequacy of CIP-014-3's Applicability criteria.

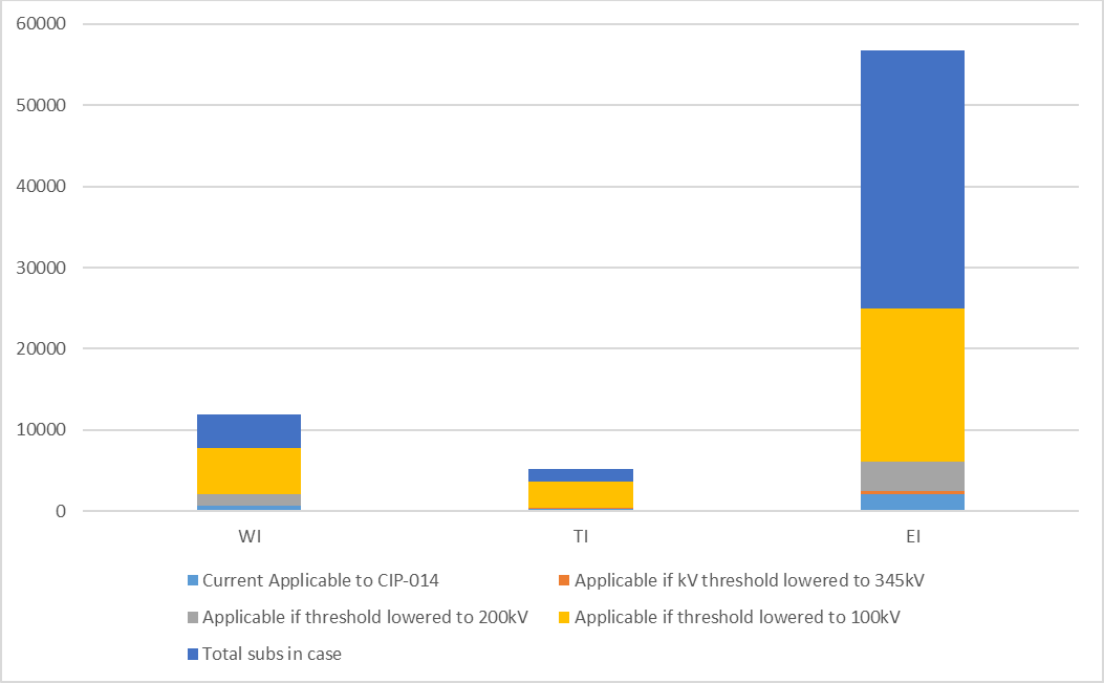

Figure 1: Substation Topology Estimates Using Planning Cases

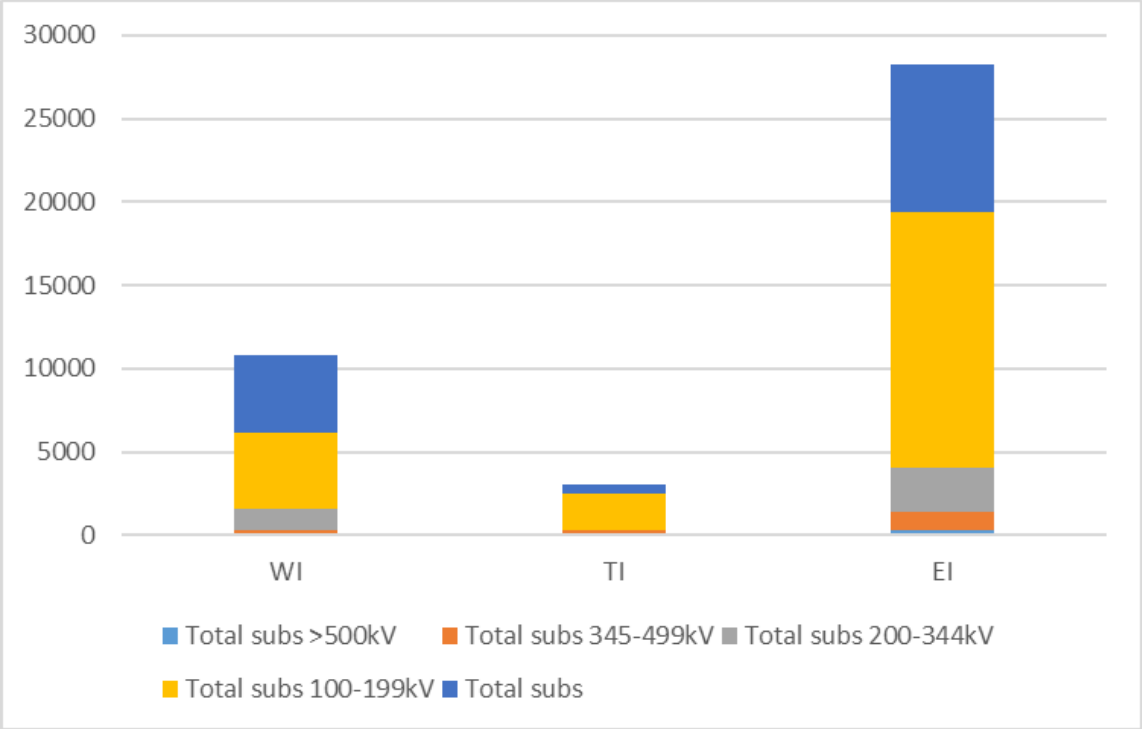

Figure 2: Substation Classification Using EIA data

Evaluation of CIP-014 Applicability Criteria

Reliability Standard CIP-014 is designed to identify those "critical" facilities that would present significant risks to the reliability of the BPS if damaged or rendered inoperable as a result of a physical attack. The expectation in the Commission's March 2014 Order directing the development of the standard was that a limited number of substations would be identified in the risk assessment as having the type of adverse impact on the Interconnection the standard was designed to mitigate. Consistent with that expectation and to help ensure that industry resources were properly focused on those Facilities that present an elevated risk, CIP-014 uses a screening approach to determine which facilities should be assessed.

NERC finds that the objective and screening approach of CIP-014 continues to appropriately focus limited industry resources on risk to the reliable operation of the BPS associated with physical security incidents at the most "critical" facilities. Based on studies using available data, NERC finds that the CIP-014 Applicability criteria is meeting that objective and is broad enough to capture the subset of applicable facilities that TOs should identify as "critical" pursuant to the Requirement R1 risks assessment. As explained below, NERC did not find evidence that an expansion of the Applicability criteria would identify additional substations that would qualify as "critical" substations under the CIP-014 Requirement R1 risk assessment. Accordingly, at this time, NERC is not recommending expansion of the CIP-014 Applicability criteria. NERC acknowledges, however, that supplemental data[15] could show that additional substations configurations would warrant assessment under CIP-014 and plans to continue such evaluation, as described below.

Analysis of Applicability Criteria

The CIP-014 Applicability criteria represent different indicators of higher potential risk to identify a subset of substations, referred to herein as the applicability list, that should be subject to the Requirement R1 risk assessment. The Applicability criteria of CIP-014 consists of four criteria, further analyzed in the sections below. These four criteria are:

- A Voltage inclusion criterion (applicability criterion 4.1.1.1);
- A weighting factor inclusions criterion (applicability criterion 4.1.1.2);
- An inclusion for Transmission Facilities that are identified by a RC, PC, or TP as critical to the derivation of an Interconnection Reliability Operating Limit ("IROL") and their associated contingencies (applicability criterion 4.1.1.3); and
- An inclusion for Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements (applicability criterion 4.1.1.4).

Voltage Inclusion Criterion

The voltage inclusion criterion brings in all transmission facilities operating at 500 kV or higher. The inclusion of all substations with 500 kV transmission facilities is an appropriate bright-line criterion for identifying a potentially critical substation.

Weighting Factor Inclusion Criterion

The criterion aligns with CIP-002-5.1a Impact Ratings for medium impact BES Cyber System (BCS), criterion 2.5. This criterion uses a combination of aggregated transmission line weighting values, as shown in **Table 2**, along with a minimum number of distinct substation connections. This criterion includes transmission facilities that are operating between 200kV and 499kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other substations and has an "aggregate weighted value" exceeding 3000.

[15] Namely, expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration.

Table 2: CIP-014-3 Line Weighting Criteria

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

NERC notes that CMEP evaluations of registered entity practices for substation applicability list development provided additional insight on different approaches for determining line counts. Unique variations of certain substations add complexity to the aggregated weighting, such as split buses, ring buses, multiple ownership configurations, and other topology variations that may need a human evaluation to ensure that registered entities correctly count lines and connecting substations. Currently, there is insufficient data regarding the extent of observed approaches that do not align with ERO Enterprise expectations and whether modifying the Reliability Standard to add clarity regarding line count methods is warranted. CMEP staff will continue to leverage the CMEP Practice Guide for CIP-014-3 R1[16] when performing compliance and risk determinations and assure CMEP program alignment.

Substations with Partial Criterion Applicability

To determine whether the weighting factor criterion is adequate to meet the objective of CIP-014, NERC looked to identify what types of substations would not fully meet this criterion but did include some partial characteristics. Initially, NERC identified a limited number of topology configurations for substations with line weightings that were close to but below the aggregated value of 3000. These topology configurations include substations with:

- 230 kV (4 or less lines) totaling 2800;
- 345 kV (1 or 2 lines) totaling 1300 and 2600 respectively; and
- 345 kV (1 line) and 230 kV (1 or 2 lines) totaling 2000 and 2700 respectively.

NERC also identified substations that could exceed an aggregated line weighting of 3000 but would not be required to be included within the risk assessment because they: 1) only connected to one or two other substations and 2) the other applicability criteria did not apply.

Based on the data available at the time of this report, NERC sought to analyze the potential impact of the loss of existing substations with these two types of partially applicable criterion (i.e., those close to but below the 3000 weighting and those over 3000 but with only one or two other connections). As explained below, using data available from CMEP activities and planning cases, NERC did not identify any instances where an entity had substations meeting these characteristics (and thus excluded from the CIP-014 risk assessment) that would have had the adverse system impacts that CIP-014 is designed to identify. While expanding the CIP-014 applicability criteria to include these types of substations would provide for a larger pool of substations to assess under Requirement R1, there is no indication that an expansion of the weighting factor inclusion criterion is warranted for the purpose of identifying additional "critical" substations.

The following is an explanation of NERC's approach to evaluating the adequacy of the weighting factor criterion. Specifically, NERC performed a preliminary screen of steady-state data as well as a sensitivity analysis. The details and results of these evaluations are included below.

[16] NERC, *ERO Enterprise CMEP Practice Guide: CIP-014-3 R1* (Sept. 2022), https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20CIP-014-3%20R1.pdf.

Steady-State Preliminary Screen

As a preliminary screening test, NERC analyzed the outage of each substation in steady-state Contingency processing tools in both a heavily and lightly loaded condition. This screen provided an indication of whether substations that fall outside of the aggregate 3000 line-weighting criteria could potentially cause the adverse impacts that CIP-014 is designed to prevent. **Table 3** demonstrates the findings of this screen. The difference between the total number of substations versus the total number of solved and unsolved Contingencies is explained by the fact that the Contingency processor did not reflect in service substations only. Thus, a number of substations identified for Contingency were skipped due to being modeled in the chosen cases as out-of-service. NERC staff counted the unique set of Contingencies between the cases, reflected in **Table 3**. NERC staff spot tested the number of not solved Contingencies and the majority were determined to be a numerical or model issue that is resolved by correcting the elements. Further, spot testing the Contingency with a transient dynamic simulation for the most overloads or voltage violations demonstrated that the system stayed stable during these extremes. The results of this steady-state preliminary screen do not indicate that modification to the applicability criteria is needed at this time. This further supports the conclusion that the substations in question are relatively smaller than those substations covered by the current CIP-014 applicability and, as such, are less likely to cause instability, uncontrolled separation, or Cascading if rendered inoperable.

Table 3: Steady-State Preliminary Screen Results

Assessment Metric	Count
Total Number of Substation Contingencies	22,514
Total Unique Substation Contingencies	11,784
Total Number Solved	17,070
Total Number Not Solved	445
Maximum Count of Overloads in a Single Contingency	8
Maximum Count of Voltage Violations in a Single Contingency	261
Number exhibiting instability, Uncontrolled Separation, or Cascading	0

A more thorough technical analysis, such as the inclusion of a dynamic study, would need to be performed in each instance to further confirm the conclusion as potential impacts will vary depending on the electrical characteristics of the connected network. Studies for substations above 3000 but with only one or two connections may already be covered by an assessment required by Reliability Standard TPL-001 as the Contingencies selected for TPL-001 include single line outages and common tower outages that include two or more lines out of service. However, TPL-001-5.1 currently does not require the evaluation of the loss of all elements within a substation to evaluate the other identified instances of partial criterion applicability. NERC will continue to assess the effectiveness of CIP-014's Applicability Criteria to determine if any of these configurations would result in a critical identified substation.

Sensitivity Analysis for Potential Scope Increase

To further NERC's understanding of the potential scope of substations subject to the CIP-014 Applicability criteria, NERC conducted an analysis to estimate the total populations of included versus excluded substations. NERC receives electric models of the Interconnection (e.g., steady-state and dynamic transient models) through the Reliability Standard MOD-032 process. NERC applied different approximated criteria alterations to these Interconnection cases to evaluate impacts and estimate the number of substations that could be applicable under different criteria.

Adjusting just the voltage applicability criteria (4.1.1.2), **Figure 3** displays the percentage of substations in the planning models that would currently be applicable to CIP-014 using the topology estimation tool and the upper bound of substations. **Table 3** separates the Western Interconnection (WI), Texas Interconnection (TI), and Eastern Interconnection (EI) into different bars in **Figure 1** for each voltage levels. These are to mirror the lower kV of the

CIP-014 line weighting criterion to determine the upper bound of applicability changes to the number of substations currently assessed per the Requirement R1 risk assessment. This demonstrates the enhanced study rigor and scope of the standard should the applicability criteria be altered to include more substations, but does not speak to if those added substations would be deemed "critical." The >100 kV section shows substations that would meet the normal BES definition cutoff.

As demonstrated in the graph, the number of substations currently applicable (per 4.1.1.1 and 4.1.1.2) is around 10 percent. Lowering the voltage applicability from 500kV threshold to 345kV keeps the percentage of applicable substations to approximately 10 percent. This is due to the fact that current CIP-014 applicability covers the large majority (>85%) of 345kV substations. To expand the substations applicability in a significant manner, the voltage threshold would need to include substations >200 kV to increase the percentage coverage of substations in a significant way (by five percent or more). Modifying the voltage applicability to include all BES represented buses would ensure 100% of all substations be applicable to the risk assessment.

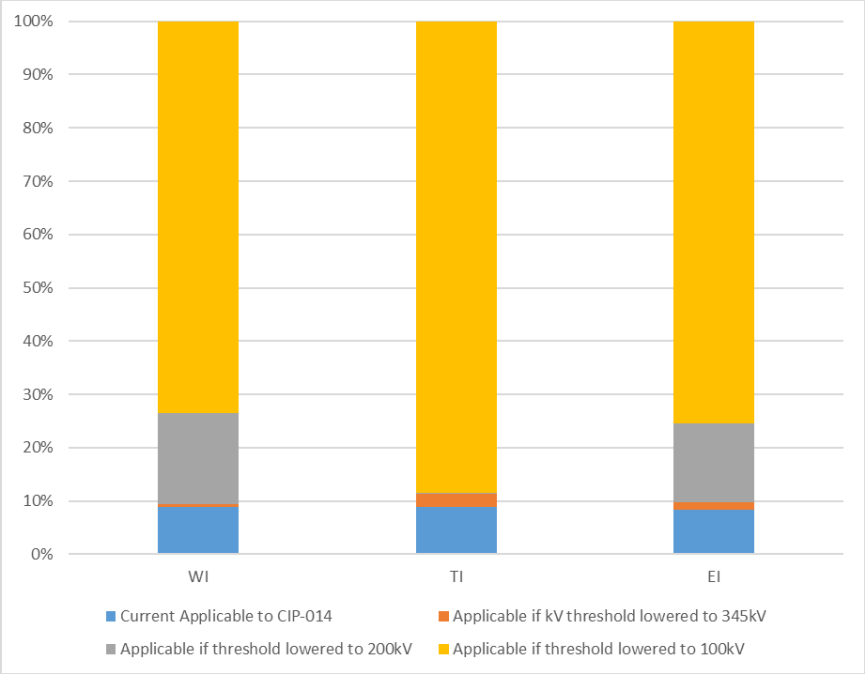

Figure 3: Estimated Percentage of Substations Applicable

The results of this sensitivity analysis do not provide any indication that modification to the applicability criteria is needed to capture additional "critical" substations. Similar to the results of the preliminary screen, determining that the applicability list includes a large enough set of the total population is challenging without conducting a full risk assessment for all stations. The justification for the CIP-014 risk-based screening approach – i.e., to study only those stations that meet a high bar of criteria – remains appropriate. As only very few of the currently studied substations are identified as critical, the screening approach continues to be reasonable. Engineering judgment will also show that the lower kV substations typically do not influence the remainder of the BPS as great as the larger, higher kV class substations. As **Figure 3** demonstrates, the kV class criterion can be altered to increase the amount of substations included in the risk assessment, but only lowering to >200kV would provide a substantial increase in the amount of substations for the study. Further, the applicability increase doesn't necessitate any of those added substations being deemed "critical" per the risk assessment as indicated previously in **Table 3**.

Based on the results of the preliminary screen and sensitivity analysis, NERC has not identified any new information that would warrant expanding or modifying the weighting factor criterion at this time. NERC plans, however, to continue evaluating the adequacy of this Applicability criterion in meeting the objective of CIP-014. NERC recognizes

that supplementary data could show that additional substations configurations would warrant assessment under CIP-014. The supplementary data would include expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration. Accordingly, NERC recommends holding a technical conference to, among other things, identify the type of substations it should study and establish data needs for conducting studies on those substations to determine whether they should be included in the weighting factor criterion. NERC plans to consult with FERC staff on the content, timing, and logistics for holding the technical conference.

Inclusion Criterion for Transmission Facilities Identified by Other Registered Entities

This criterion in CIP-014's Applicability provides additional assurance that registered entities with other functional obligations to study adverse impacts to the Interconnection have direct input to the applicability list for CIP-014-3. There is a standard development project in progress addressing potential changes to language in CIP-002 and CIP-014 to clarify these roles and tasks. NERC Reliability Standard Project 2021-03[17] addresses the responsibility of RC, PC, and TPs in identifying Facilities that warrant CIP-014-3 consideration; specifically to address TPs and PC functions language relating to inclusion of Facilities critical to the derivations of IROLs.

As stated in the NERC 2022 CMEP Implementation Plan,[18] NERC and the Regional Entities conducted a joint review with RCs to understand how RCs are performing their analysis and determining IROLs, including how the RCs incorporate the recommended practices outlined in NERC *Reliability Guideline – Methods for Establishing IROLs*.[19] The results of this IROL joint review are not publicly available at the time of this report. NERC intends on sharing the results with the Project 2021-03 Standard Drafting Team to consider during the standards modification process.

Note that if a TO completes CIP-014-3 R1 risk assessment and found no stations that meet the criteria specified in Applicability Section 4.1.1, the TO doesn't have a requirement to conduct another risk assessment for the next 60 calendar months. If the RC/PC/TP declares the station as critical to the derivation of an IROL and its associated contingencies after the TO has completed its risk assessment, the TO still does not have to do another assessment until its 60 calendar months mark. This offset on the periodicity of the R1 risk assessment based on CIP-014 Applicability changes is discussed more in the evaluation of the R1 risk assessment where NERC recommends an alignment of this periodicity. This issue, however, is not an indication of altering the scope of applicable Facilities but on how often they are studied in Requirement R1.

Inclusion Criterion for Transmission Facilities Meeting Nuclear Plant Interface Requirements

The inclusion criterion for those Transmission Facilities meeting Nuclear Plant Interface Requirements is an appropriate threshold for a identifying a potentially critical station.

Impact Assessment of Recent Attacks on Applicability

Recently reported physical attacks resulted in the loss of end-use customers and the ability to serve load through a portion of the high voltage network. These attacks, however, did not result in instability, uncontrolled separation, or Cascading. Specifically, NERC determined that substations attacked in Moore County, North Carolina that the December 15 Order references would not have been covered by the CIP-014-3 applicability. The referenced attack left multiple geographically close substations damaged, resulting in the loss of end-use customer load. Based on the topology, the substations attacked do not meet the line weighting for the applicability list. The attack rendered one BES substation inoperable and did not result in instability, uncontrolled separation, or Cascading for the Interconnection. These facts about the attack indicate that even if the substation were subject to Requirement R1

[17] The Project 2021-03 – CIP-002 Communications Protocol Converters webpage is available at https://www.nerc.com/pa/Stand/Pages/Project%202021-03%20CIP-002%20Transmission%20Owner%20Control%20Centers.aspx.

[18] NERC, *2022 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan* (Oct. 2021), https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20CMEP%20Implementation%20Plan%20v1.0%20-%202022.pdf.

[19] NERC, *Reliability Guideline – Methods for Establishing IROLs* (Sept. 2018), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf.

risk assessment, the loss of the BES substation in the attack would not result in instability, uncontrolled separation, or Cascading. Placing CIP-014 type physical protections on those stations that do **not** cause instability, uncontrolled separation, or Cascading is not consistent with CIP-014's purpose of identifying and protecting the substations that would cause instability, uncontrolled separation, or Cascading. Physical protections against these types of attacks is covered later in this report discussing minimum physical security protections for all BPS substations.

Adequacy of Applicability Criteria Conclusions

In sum, based on available data, the Applicability criteria in Reliability Standard CIP-014-3 appears to adequately identify the subset of all transmission stations and substations that TOs should evaluate as part of the Requirement R1 risk assessments. A large majority of those stations currently studied in the risk assessments will not be identified as critical and there are no current studies that indicate an expansion of the Applicability criteria will identify additional stations that would qualify as "critical substations" under the Requirement R1 risk assessment.

NERC will continue to assess and conduct oversight of CIP-014-3 implementation around applicability list development and maintenance. NERC will also conduct engineering assessments to ensure the applicability is effectively covering the various configurations of transmission substations. Along with the recommendations to hold a Technical Conference for minimum level of security, NERC will, among other things, establish additional study and data needs to confirm its analysis as demonstrated in this report. More details on the recommended Technical Conference are found in the section **Evaluation of Minimum Level of Physical Security Protections.**

Evaluation of Requirement R1 Risk Assessment Adequacy

Analysis

The CIP-014 Requirement R1 risk assessment requires applicable TOs to study whether the loss of an applicable substation could result in instability, uncontrolled separation, or Cascading. While the objective of these assessments is appropriate, NERC finds that there should be additional clarification as how registered entities must conduct the assessments. In reviewing its CMEP data, NERC found that registered entities have inconsistent approaches to performing the risk assessment and they did not always meet the technical rigor expected for other planning horizon study assessment-related Reliability Standards, such as TPL-001. This report aggregates the issues identified to date for risk assessment adequacy by 1) deficiencies introduced into the models[20] used within the risk assessment, and 2) insufficient technical studies, including insufficiently documented technical rationale.

Risk Assessment Deficiencies Caused by an Entity's Model Decisions

While the Requirement R1 risk assessment is applicable to TOs, not all TOs have in-house SMEs to conduct the studies. TOs are largely aware of their own assets and can identify nameplate information, cybersecurity impacts, and applicability inside the boundaries of their substations. However, while the TO may be an expert in identifying their equipment and its location, TOs often lack in-house expertise to study Interconnection-wide electrical impact, which requires specific tools, data, and analysis of simulation outcome. Collectively, these issues complicate a TO's thorough understanding and review of modeling decisions and justifications made by other entities responsible for model curation such as TPs and PCs. Further, CMEP personnel have identified that these modeling decisions do not apply consistent engineering practices and often either introduce inappropriate future projects or apply inappropriate study periodicity.

Inappropriate Future Projects

Based on ERO stakeholder engagement and CMEP observations, many TOs have been seeking clarity regarding how the risk assessment window for the initial and subsequent assessments overlapped with projects considered in-scope for the risk assessment. As a registered entity leverages Interconnection-wide base cases to perform the CIP-014-3 Requirement R1 risk assessment, the base case availability plays a part in a registered entity's responsibilities.

Applicable registered entities are required to perform the CIP-014-3 Requirement R1 risk assessment at least once every 60-calendar months or 30-calendar months, depending on whether or not the previous risk assessment identified any critical substations. Risk assessments are required to include existing substations and those planned to be in-service within 24 months of the risk assessment. This indicates that there are two paths taken based on the outcome of the R1 risk assessment. The two paths are as follows:

1. If the assessment for in-service equipment 24 months in the future designates at least one critical substation, conduct the next risk assessment within 30 months, and
2. If the assessment for in service equipment 24 months in the future designates no critical substations, conduct the next risk assessment after 60 months.

A registered entity has the flexibility to conduct this 24-month look ahead risk assessment on a more frequent basis. However, the Interconnection-wide base cases typically are built on an annual frequency causing additional complexity. It is unlikely that more frequent risk assessments will produce differing results due to the base case creation timelines. **Figure 4** graphically illustrates the timeline between the end of the risk assessment and the next time a registered entity is required to perform a subsequent risk assessment.

[20] "Models" herein refer to the aggregated set of electrical components and characteristics used by power flow software programs to: 1) evaluate and monitor Real-time conditions, 2) evaluate the efficacy of planned system changes for Transmission, generation, and forecasted changes to demand/load, and 3) simulate Contingencies such as events, severe weather, faults, etc. to test the resiliency of the area studied.

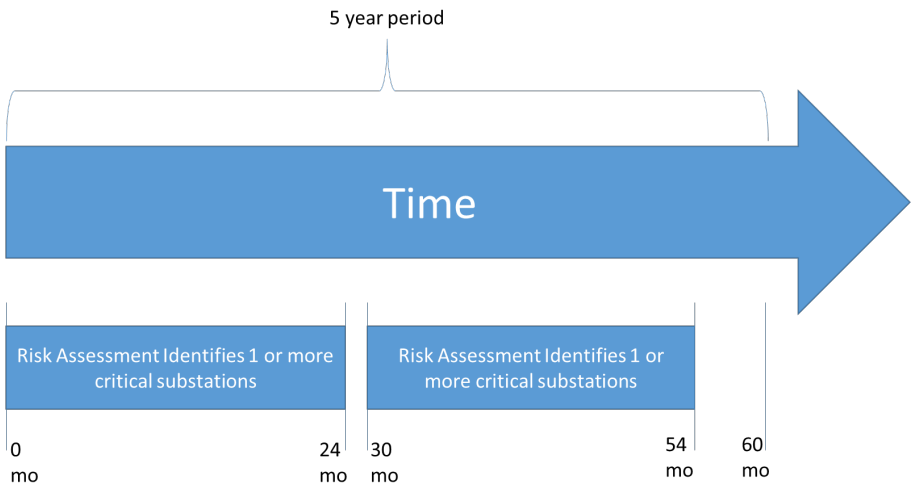

Figure 4: Current CIP-014 R1 Risk Assessment – Using 30 Months

CIP-014-3 requires that a registered entity must include projects that will be in-service within the next 24 months but does not provide a full-time range of acceptable projects to include. For example, in the case of the 30-month frequency of study, TOs are often provided a 5-year model by their TP or RC.[21] The result of the registered entities having the 5-year model allows it to include projects that the TP or RC have projected be in-service for dates beyond the next two risk assessments. CMEP staff often observe the inclusion of these projects during CMEP activities and through NERC Oversight.

There is a different concern when there are no critical substations identified during the previous risk assessment, as shown in **Figure 5**. As a result, this introduces a potential that the risk assessment fails to include all in-service projects through the full time period between risk assessments. In both cases, the ability to effectively and consistently identify critical stations within the 5-year horizon may be negatively impacted.

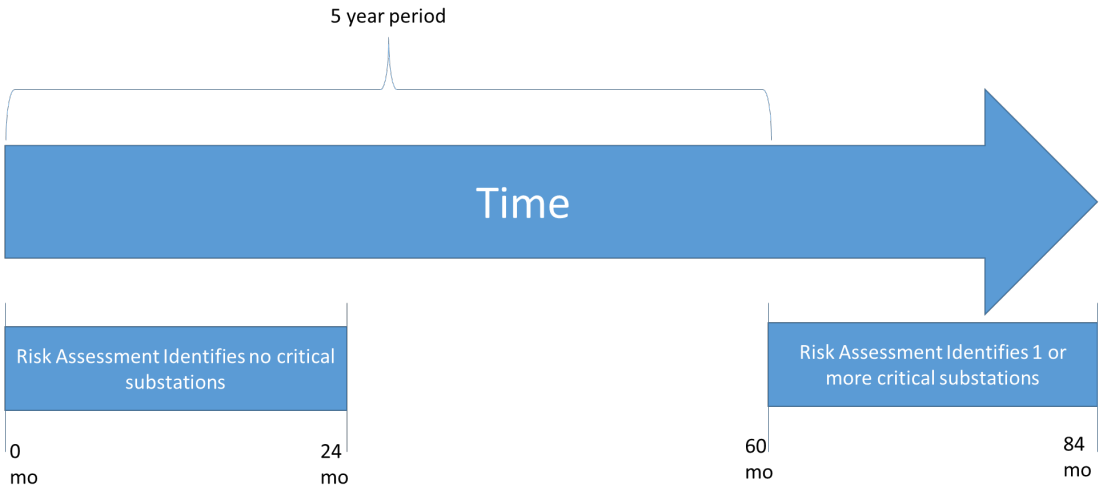

Figure 5: Current CIP-014-3 R1 Risk Assessment – Using 60 Months

[21] Within transmission planning studies, a 5 year (or 60 month) period is generally used to scope the Near-Term Planning Horizon.

A TO may conduct more frequent risk assessments, but the obligation allows for a 30-month periodicity when a TO identifies a critical substation. Per the technical rationale for CIP-014:[22]

> The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates.

Each TO is required to submit their expected in-service projects for the Interconnection-wide models used to assess the stability of the Interconnection. It is during that stage that surrounding TO projects are included.

Further, this technical rationale refers to the planning cycle and frequency that a TO constructs substations. This is dissimilar from how TPs build models to conduct long-term planning assessments. This introduces discrepancies in decisions made regarding the use of models and what the registered entity considers appropriate to include within the study and the number of years studied.[23]

Inappropriate Study Periodicity

CIP-014-3 periodicity is different between registered entities that do not have critical identified substations and those that have previously identified critical substations. The CIP-014-3 Requirement R1 risk assessment must evaluate impacts to the Interconnection that necessitate the need for models used during each registered entity's risk assessment to include up to date models of neighboring systems. While a registered entity may not have identified critical stations in their footprint, the modification of the system in future years may result in changes to system flows that could influence risk assessment results. As the periodicity between neighboring registered entities may be different (up to 30-60 months), there may be a gap in risk assessment efficacy during years project update data does not overlap with study periods.

A risk assessment conducted without this update to surrounding facilities can influence the quality of the assessment as facilities not in-service pose challenges with conducting the risk assessment and the quality of the assessment's results. While the technical rationale for this flexibility is appropriate for a single TO, it does not effectively apply to all areas where surrounding transmission buildouts may influence the remainder of the interconnected system. For this reason, registered entities should understand and mitigate the allowable 6 month to 36-month[24] reassessment delay.

Registered entities must mitigate the issues presented by risk assessment modeling decisions to require when a critical substation is identified within a planning footprint to assess the impact of the project. One method to accomplish this is to require areas that have identified critical substations to consistently assess the impact of their and neighboring facilities have on the loss of the identified critical substation. One example of how registered entities can consistently assess the impact of critical substations is by lowering the 30-month window to 24 months as shown in **Figure 6**. This method would alter the quantity of assessments performed by registered entities; however, the alteration is minor.[25] This is not the only way to make the timelines consistent with project submittals and updates to transmission in a registered entity's footprint. Registered entities should explore alternative options to ensure alignment of the risk assessment cycle and a systematic project update for surrounding TOs.

---

22 CIP-014-3 is available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf.

23 Transmission Planners are required to annual study forecasted system changes for Year 1 (or Year 2) and Year 5 at a minimum. Planners will often study additional future years depending on their own practices and system needs.

24 Should a neighboring set of two entities not have critical facilities, the period gap between the end of the risk assessment period (24 months) and the subsequent risk assessment (at 60 months) is 36 months total of potential transmission assets not assessed for their potential impact or identification of critical substations.

25 Mathematically, over a 10 year period this increase is one extra study.

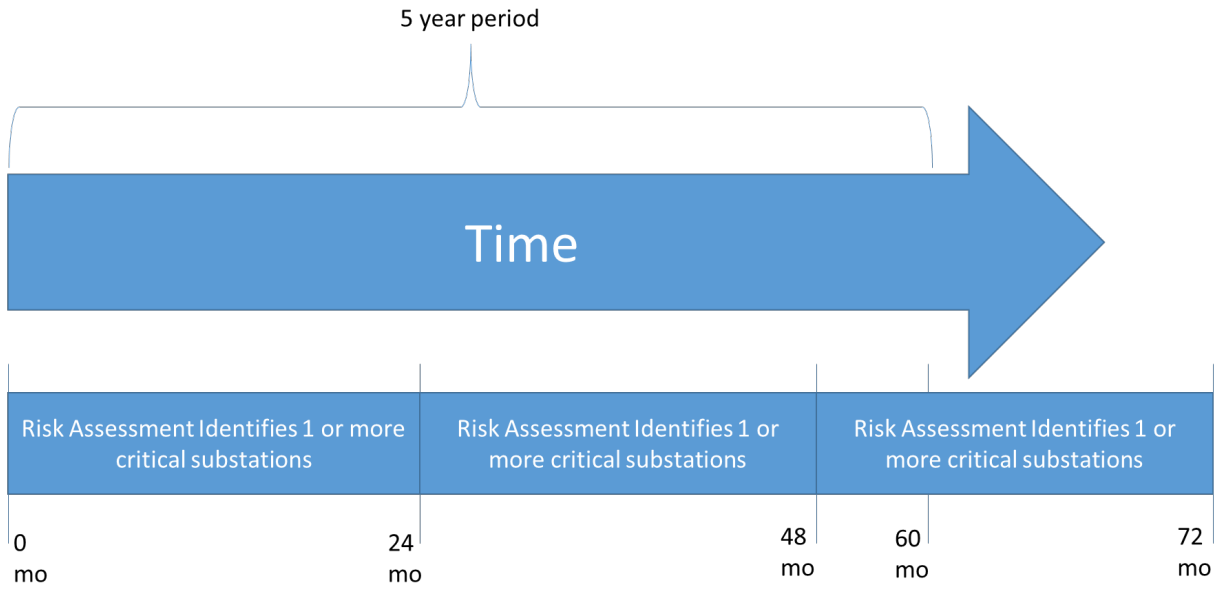

Figure 6: Example of Resolved Risk Assessment Periodicity

Insufficient Technical Studies Including Insufficiently Documented Technical Rationale

To accomplish the risk assessment, TOs are required to use models to simulate and evaluate the loss their equipment poses to the Interconnection. TO's substantiate these risks by evaluating electrical responses for violations of different criteria used in the study of instability, uncontrolled separation, or Cascading. Determinations of effective and sufficient criteria necessitate technical expertise. The accuracy and validity of model data, operational studies, and long-term studies are often the subject of NERC reliability guidelines, alerts, and CMEP activities. TOs that are not also regularly involved in TP studies and current reliability concerns are unlikely to provide the most assurance of the efficacy of any given study. Further, study efforts by the TO are duplicative, as it is also the responsibility of a TP to identify projects and ensure reliable operation of the BPS years into the future.

The ERO Enterprise finds that the technical rationale provided by registered entities is frequently insufficient to demonstrate compliance with the CIP-014 Requirement R1 risk assessment.[26] Audits of CIP-014 frequently do not contain sufficient technical rationale by registered entities that fully supported registered entity decisions and methods for evaluating instability, uncontrolled separation, or Cascading. Sufficient and clear guidance on how to study instability, uncontrolled separation, and Cascading have been available to registered entities in NERC Reliability and Security Guidelines.

From the CMEP Practice Guide for CIP-014-3 R1:

> The language within CIP-014-3 does not prescribe a specific method on how each risk assessment of the entity's Transmission station(s) and Transmission substation(s) shall be performed. As such, specific components that comprise any supporting analytics are neither defined nor listed. This provides intentional flexibility for various approaches to the CIP-014-3 R1 risk assessment, due to the expected differences in each individual entity's facts and circumstances. However, that flexibility does not alter R1's language that each risk assessment *must* be "designed to identify" which applicable Transmission station(s) and Transmission substation(s), that if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection. Entities may implement different approaches to complete this objective, but the approach must be able to accomplish the fundamental obligation of requirement through effectively assessing all required adverse system conditions with sufficient supporting technical analyses.

[26] NERC CIP-014-2 Peer Review Team – Consensus of CMEP Gap; March 15, 2021.

A recent *Reliability Guideline on the Methods for Establishing IROLS*[27] contains the various studies, time domains, and key recommendations to determine the limits substations can take before instability, uncontrolled separation, or Cascading occur. To ensure that no instability occurred in simulation, registered entities can cover each broad type of stability analysis (e.g., frequency or rotor angle) via Contingency analysis, governor power flow analysis, and transient stability analysis; as shown in **Figure 7**. While NERC considers that it would be very difficult for an entity to demonstrate a risk assessment which effectively evaluates instability without performing a dynamics analysis, there is consensus that more specific language to the R1 requirement would add clarity. ERO Enterprise CMEP findings further substantiate that additional clarification in the risk assessment requirement would benefit registered entities in sufficiently assessing instability, uncontrolled separation, or Cascading.

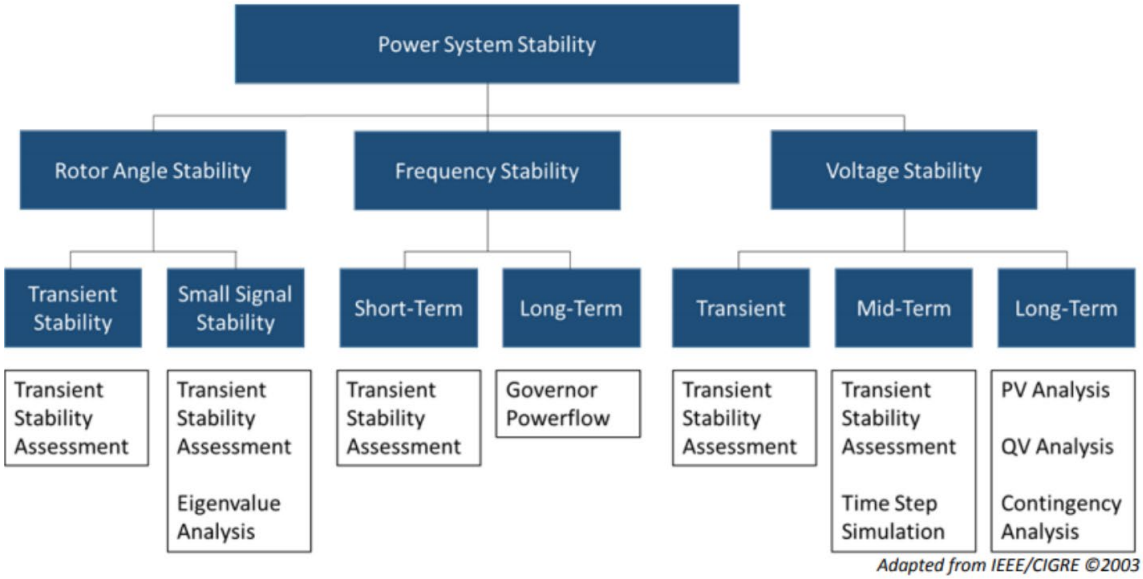

Figure 7: Generic Overview of Power System Stability

The technical rationale included in CIP-014-3 lists a few different example criteria to weigh the electrical impact for a particular Contingency (i.e., the loss of a transmission substation) among which include TPL-001 R6, EOP-004, and impact area. According to the technical justification, the registered entity "has the discretion to choose the specific method that best suites its needs. As an example, a registered entity may perform a Power Flow analysis and stability analysis at a variety of load levels." The variety of what study criteria may be most appropriate for a registered entity's facts and circumstances supports the benefits of built-in flexibility in requirement language for the risk assessment. For instance, some registered entities added facilities identified as part of IROL to the potential list of criteria, which carries with it the SOL Methodology found in FAC-014-2.[28] However, ERO stakeholders have identified that the variety of criteria used in the risk assessments is not always the most appropriate to effectively evaluate instability, uncontrolled separation, or Cascading. As such, the ERO Enterprise agrees that CIP-014-3's risk assessment should be clarified in establishing the criteria used in the risk assessment to measure instability, uncontrolled separation, or Cascading.

[27] NERC, *Reliability Guideline: Methods for Establishing IROLs* (Sept. 2018), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf.

[28] Reliability Standard FAC-014-2 – Establish and Communicate System Operating Limits, https://www.nerc.com/pa/Stand/Reliability%20Standards/FAC-014-2.pdf.

Severity of Case

Registered entities design risk assessments to be flexible enough to gather the necessary data and perform an analysis that suits its local facilities. However, collaboration with ERO stakeholders have identified that while flexibility covers instances of high stress on the in-scope substations, it is not clear that the risk assessment requires registered entities to use models that correlate to periods of high flows or high stress on their system. Typically, registered entities in the NERC footprint are either winter peaking or summer peaking. These peak conditions historically have been associated with times of higher stress on the transmission system and a higher likelihood that a registered entity reaches its stability margin. As physical security attacks may be planned events, CIP-014-3 risk assessments should seek to evaluate conditions during the most stressed of conditions. Implementing best practices in the case of CIP-014-3 is in line with the standard's purpose and these more potentially severe threats.

Through collaboration with ERO stakeholders, NERC has identified that the term "inoperable or damaged" may leave registered entities too much flexibility when determining study criteria. NERC has verified during multiple oversight activities that registered entities often do not study a more severe failure. Many registered entities have found that the term "inoperable" includes the total loss of communication and protection equipment at the substation, necessitating delayed clearance from far-end relaying to isolate the event's impacts. Damaged substations may be able to self-isolate, and thus would indicate a normal clearing time. Reliance on local relays at the substation that is also under attack should not be permitted. Clarifying this issue could assist in a "worst case" risk assessment versus a design scenario for security professionals to perform a Design Basis Threat ("DBT") analysis to mitigate the "worst case" of the substation being rendered inoperable or damaged.

Physical Proximity Determinations

The CIP-014 R1 risk assessment differs from most other transmission planning studies in that the registered entity must consider physical proximity regardless of electrical connection, as the CIP-014 assessment requires the entire transmission station to be put into an outage rather than just particular elements inside the substation. An example of the type of factors to consider when assessing close proximity is where proximity is defined as having two or more substations situated such that one or more of the following apply:

- An easy line-of-sight between the entire substation yards from a single site.
- An easy access from a common public roadway that exists between all of the substation yards.
- The substation yards are in close enough proximity that a single event can impact both substations (e.g., the debris field from an incendiary device set off at one yard will impact the other yard).

The ERO Enterprise identified areas of concerns in the inconsistent application to determine the proximity of substations for determining CIP-014-3 the assessment. Debates on inclusion or exclusion of this equipment for the Contingency definition typically occur when two or more substations are within eyesight of each other or if they are jointly owned substations. Reliability Standard CIP-014-3 does not set distance requirements or outline other factors for determining whether there is a single substation or multiple substations for applicability or risk assessment purposes. Regional Entity stakeholders agree that there is a need to clarify how registered entities should account for physical proximity when defining the Contingency to input a CIP-014 applicable facility into the R1 risk assessment, such as when substations are within line-of-sight of each other. Registered entities that develop and can demonstrate a consistently implemented method for determining physical proximity would be considered a best practice.

Guidance and training to CMEP staff include evaluating methods used for determining physical proximity issues. CMEP staff may choose to conduct site visits during their fieldwork to substantiate registered entity-applied methods or to perform verification in cases where physical proximity determinations are unclear. NERC recommends that a SAR that clarifies this Contingency definition be included in the enhancements to the R1 risk assessment.

Adequacy of Risk Assessment Criteria Conclusions

As described above, ERO Enterprise CMEP activities indicate that while the overall objective of the Requirement R1 risk assessment is sound, there are inconsistent approaches to the risk assessment. The ERO Enterprise observed that in certain instances registered entities failed to provide sufficient technical studies or justification for study decisions. This has resulted in instances of noncompliance, such as when registered entities were unable to sufficiently substantiate the risk assessment. The inconsistent approach to the requirement is likely impacted by a lack of specificity in the requirement language as to the nature and parameters of the risk assessment.

Given NERC's finding regarding the inconsistent application of the Requirement R1 risk assessment, NERC will initiate a Reliability Standard Development project to evaluate changes to provide additional clarity on the risk assessment. NERC recommends the following:

- Clarify the risk assessment methods for studying instability, uncontrolled separation, and Cascading, such as the expectations of dynamic studies to evaluate for instability.
- Clarify the case(s) used for the assessment to be tailored to the Requirement R1 in-service window and correct any discrepancies between the study period, frequency of study, and the base case a TO uses.
- Clarify the documentation, posting, and usage of known criteria to identify instability, uncontrolled separation, or Cascading occur as part of a risk assessment. The criteria should also include defining "inoperable" or "damaged" substations such that the intent of the risk assessment is clear.
- Clarify the risk assessment to account for adjacent substations of differing ownership, and substations within line-of-sight to each other.
- Clarify that the risk assessment should simulate the complete loss of a Transmission station or Transmission substations that includes the simultaneous loss of all station elements and a does not rely on local system protection for relay clearance.

Evaluation of Minimum Level of Physical Security Protections

As discussed below, while NERC is not recommending an expansion of the CIP-014 Applicability criteria at this time, NERC finds that, given the increase in physical security attacks on BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks to the BPS associated with physical security attacks. Due to a high degree of public interest regarding physical security following the recent substation attacks, there has been a greater amount of discussion regarding how attacks are mitigated through successful implementation of NERC Reliability Standards. There has also been some confusion regarding some of the discussions points within the public narrative as CIP-014 is inferred to be the measure to prevent all physical attacks and mitigate their associated impacts. This section first discusses the analysis of event data NERC is using in this report and the physical security threat landscape. This information is important to consider when addressing proper security risk assessments.[29] Second, this section outlines how physical protections are uniquely designed and implemented to accomplish specific objectives and are not uniform or interchangeable. Third, this section discusses what physical security threats are applicable to CIP-014, which ones are not, and why the distinction is important. Finally, this section concludes our assessment that a determination of any minimum level of protections requires a larger, coordinated, and collaborative effort to mitigate the impact of physical attacks on BPS substations, including those that fall outside of CIP-014 applicability.

Analysis of Physical Security Event Data

To support the evaluation of reported physical security events, E-ISAC SMEs helped outline the threats and risks facing the electric industry, and provided analysis of the supporting data. The E-ISAC collects physical security incidents through a variety channels. The majority of the information received is provided through voluntary means, including E-ISAC Portal posts, direct sharing by members, as well as through government partners. The other type of sharing is through mandatory reporting, which is a U.S. federal government requirement. Mandatory reports are shared with the E-ISAC for situational awareness purposes only.

Known Limits of Event Data

Due to the voluntary nature of information sharing with the E-ISAC, specific details involving potential motives, identification of suspect(s), criticality of substations and other attributes are often unknown. The E-ISAC encourages members to share any security-related information involving their assets or personnel to help ensure the E-ISAC data set is as accurate as possible in order to provide higher accuracy trend analysis on potential emerging threats to the electricity industry. NERC is unable to evaluate these trends beyond what the E-ISAC and industry provide. For instance, while reported physical security events have increased, this is still an incomplete data set. Meaning that NERC is unable to verify the completeness of the data or to what extent any increase in reporting aligns with an increasing number of events. As details of the events were aggregated, more specific information, such as system conditions at the time of the event (e.g., if the system was operating in a stressed state), are often not available.

A variety of different threat actors and violent opportunists will continue to attempt physical attacks on grid infrastructure. These continuing threats are well documented in industry alerts and publications from E-ISAC, DHS / CISA, and others. To address this ongoing threat landscape, E-ISAC members are encouraged to maintain a heightened awareness of suspicious activity around their facilities, and the E-ISAC continues to monitor activity or trends pertinent to the electricity industry, along with changing tactics, techniques, and procedures (TPPs) used by malicious actors against the grid. Based on the fluidity of the current threat environment, the E-ISAC's assessment represent a living analysis that may change and will be updated to reflect any new pertinent developments. The evaluation in this report is thus based on the information available to NERC at this time.

[29] Note that these security risk assessments are different from the R1 risk assessment that is focused on the electrical impact rather than the tactics, techniques, and procedures associated with a physical attack.

Types of Physical Events

While there are some known limits to available data, the impacts of evaluated physical security event data represent a period of heightened threat to end-use consumer load. According to a recent analysis conducted by the E-ISAC, the amount of physical security incidents which have resulted in some sort of measurable outage (i.e., loss of end-use consumer load) have increased by 71% since 2021 and 20% since 2020. **Figure 8** shows the quantity of these incidents since 2020. It should be noted that an outage in this trend indicated at least one customer was impacted as a result of the physical security incident. The data show that the rise of events resulting in one or more customers out of service vary in size, scope, and attack vector. Importantly, of the data reviewed, there have been no outages reported from a physical security event that have also adversely impacted the reliable operation of the BPS.

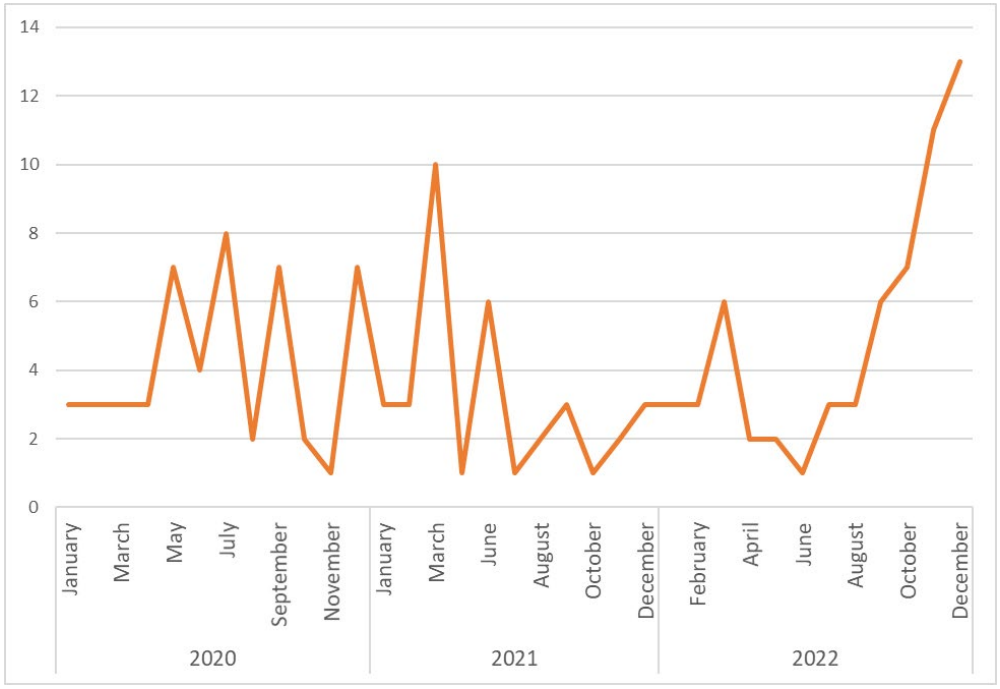

Figure 8: Quantity of Physical Security Events with Some Loss of Load for 2020–2022 [Source: E-ISAC]

The increase in **Figure 8** from 2021 to 2022 is driven by an uptick in ballistic damage, intrusion (tampering), and vandalism incidents. The smaller increase from 2020 to 2022 is due to the high number of reported incidents that occurred during 2020 that can be attributed to the onset of COVID, increased social tensions, and a decline in economic conditions. Of the total amount of physical security incidents shared with the E-ISAC during this timeframe, the vast majority resulted in no disruption to electric service (97%), and the remaining 3% resulted in varying levels of localized impact to end-use consumer load. The impacts of these events vary due the different types of physical threats that occurred as well as the facts and circumstances of the targets, including system topology, system conditions at the time of the event, and other site-specific factors.

A clear understanding of potential impacts from physical attacks is an important aspect of the evaluation in this report as effective protection measures cannot be evaluated without first having a clear objective of what threat and potential impact the security measures are meant to protect against. This data indicates that while there are a number of events corresponding with some loss of end-use consumer load, there are insufficient details to determine the scope of the impact (such as number of impacted end-use consumers over a period of time) and how to project that into potential "worst case" scenarios for that type of threat. NERC is unable to identify from this data what physical security measures were in place at substations that experienced a localized impact nor if any other specific protective measures would have uniformly prevented the impact.

Physical Security Fundamentals

While understanding potential impacts from a physical threat is necessary to outline the objective(s) of new protective measures, not all protective measures are the same or are interchangeable. In order to have a clear basis for what physical security protective measures will be effective at accomplishing the objective, a thorough risk assessment is necessary.

Design Basis Threat Risk Assessments

Physical security subject matter experts agree that risk assessments are a vital first step in determining the effectiveness of physical security measures and associated risk reduction values of those measures. Conducting risk assessments also supports an overall sound risk-management framework, which assists in enabling a structured approach to risk mitigation that can be used by asset owners and operators ("AOOs"). Risk assessments, like that required by CIP-014-3, Requirement R4, also provide assurance of a documented, iterative, and continuous approach to the physical security risk-management process that is critical to the ongoing identification and mitigation of risks.

Realistically, preventing all physical attacks is not feasible when weighed against meaningful risk reduction. Physical security controls that go beyond any identified minimum level of physical security, such as those expected to protect against coordinated or sophisticated attacks on critical infrastructure, should be based on many factors including site criticality, mean time to recovery, and other organization-specific attributes. These factors should be determined through physical security risk assessments to evaluate and define an appropriate selection of physical security protections on a case-by-case basis, as selections appropriate for one site may provide negligible reduction of risk or not be applicable at another. An example of unequal physical protections can be seen by comparing transmission substations versus transmission towers supporting the lines entering that substation. Avenues of approach to a substation are not as varied as those extending along the transmission circuit based on the terrain covered by the circuit impacting the effectiveness of some security controls. These distinctions would be a factor when performing a DBT risk assessment. A DBT risk assessment accounts for the motivations, capabilities, and tactics of potential adversaries who might attempt a physical attack.

Implementation of the Risk Assessment

The E-ISAC's Physical Security Advisory Group ("PSAG") developed guidance to provide instruction on using a DBT risk assessment for the protection of the physical infrastructure of the BPS to prevent instability, uncontrolled separation, or Cascading. Methods of implementing a DBT risk assessment, such as Vulnerability of Integrated Security Analysis ("VISA"),[30] are available to provide guidance to practitioners.[31] The VISA method looks at the security functions of detection and assessment, delay, and response, shown in **Figure 9,** and assesses them against a given threat to determine the overall effectiveness of a physical protection system ("PPS") and to evaluate cost-effective upgrades. To assist in categorizing different types of protective measures, each part of a PPS can be broken down into people, procedures, and equipment.

[30] Available on the E-ISAC Portal at: https://eisac-portal.force.com/eisacportal/s/article/134080-Vulnerability-of-Integrated-Security-Analysis-Implementation-Guide--2021-Update.

[31] The threat against which an asset must be protected and upon which the protection system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand.

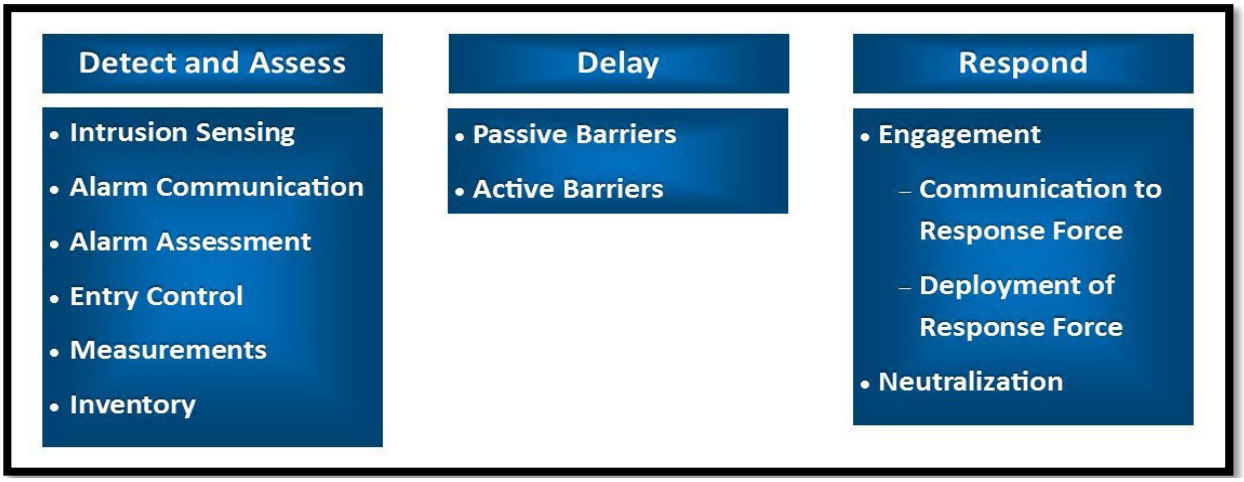

Figure 9: Three Main Functions of a PPS

Further, ongoing research and design are improving the value of each of these parts with each being an important feature when considering potential upgrades to a registered entity's PPS. Existing resources by the E-ISAC include assistance in the construction of a PPS resulting from the DBT process. These include the recently released *Physical Security Resource Guide for Electricity Asset Owners and Operators*,[32] which is available on the E-ISAC portal.

Adaptability by Design

There are a variety of physical security measures, procedures, and actions that asset owners and operators could consider utilizing as part of their operations. As previously discussed, measures are not interchangeable and cannot be expected to provide the same level of protection at all locations or for all threats. Because resources and requirements vary significantly based on a site's size, physical configuration, function, and external factors, implemented physical security protections should be flexible in order to effectively adapt to a changing threat landscape. When determining measures that address asset-specific actions, NERC recommends utilities consult with relevant stakeholder groups, including, but not limited to, management, security, legal, and human resources. In addition, NERC recommends utilities consult relevant authorities, including, but not limited to, laws, regulations, guidelines, corporate protocols, and relevant best practices.

Existing resources, such as the Suggested Protective Measures for Alert Periods,[33] includes suggested adaptive measures that may be implemented during periods of increased alert or threat. These suggested measures represent a compilation from government bodies, private entities, and independent sources and are available for additional consideration when building adaptability into a physical security design process.

Government Mandated Measures

Another factor to consider when identifying what protective measures to incorporate is that industry may be required to include other physical security protections in response to state or Provincial governmental regulation. Recently lawmakers in various U.S. states are proposing regulation to protect substation assets,[34] or have already begun implementing these processes in some instances.[35] These protections demonstrate that others in the space are working on solutions to address physical security attacks on electric infrastructure. As such, collaboration with

[32] Available at: https://eisac-portal.force.com/eisacportal/s/article/E-ISAC-Physical-Security-Resource-Guide-January-2023.

[33] Available on the E-ISAC Portal at: https://eisac-portal.force.com/eisacportal/s/article/127365-Suggested-Protective-Measures-for-Alert-Periods.

[34] For instance, this bill in S.C.: https://www.scstatehouse.gov/billsearch.php?billnumbers=3577&session=125&summary=B.

[35] Cal. Pub. Utilities Comm'n., Physical Security of Electric Infrastructure (R.15-06-009), https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/physical-security-of-electric-infrastructure.

government officials will assist in optimizing further proposed requirements and assist in preventing overlapping compliance burdens while still maintaining a strong security posture of the electric ecosystem.

Physical Security Threats and Purpose of CIP-014

This report draws a clear distinction between physical security threats that are considered within the scope of the CIP-014 Reliability Standard and those outside the scope of CIP-014. Each Reliability Standard contains a purpose statement to assist in directing the focus of development and implementation of the Standard. These purpose statements are comprehensive to address a particular risk or set of aggregated similar risks while the Reliability Standard requirements are focused directives in support of that purpose and are each crucial to achieve the Standard's purpose. As previously stated, the purpose of CIP-014 is to identify and protect those substations and their associated control centers that if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection. CIP-014 intentionally focuses on assuring protections are in place for these critical substations and associated control centers as reliable and secure operation of the Interconnection is paramount to assure all other aspects of NERC's mission are achievable.

Within the Scope of the CIP-014 Purpose

The identification and protection of critical substations and their associated control centers, includes extensive risk assessments, threat assessments, and implementation of resulting plans that provide the highest degree of technical focus and reduction of risk at individual locations. It is unclear that establishing a minimum of physical security protections for critical substations and their associated control centers provides a substantive benefit to reliability as these stations already undergo site-specific threat assessments under CIP-014-3, Requirement R4. Additionally, establishing any specific protective measures may potentially introduce contradicting compliance obligations with the Requirement R4 threat assessment. Further, any potential expansion of the CIP-014 requirements that does not improve upon or close reliability gaps regarding the standard's purpose statement detracts from that goal and may instead reduce the effectiveness of the Reliability Standard overall. Thus, NERC does not recommend modifications to the purpose statement of CIP-014 to address risks posed by the increased number of attacks at non-critical substations.

Outside the Scope of the CIP-014 Purpose

Evaluating whether to extend physical security protection requirements to substations and primary controls outside the scope of CIP-014 necessitates a larger conversation regarding threats and objectives. As outlined in earlier sections, physical security protections cannot be evaluated for potential effectiveness unless they are designed against specific threats, incorporate specific risk reduction objectives, are site-specific, and implemented through an adaptable risk framework. At this time, NERC is unable to make a determination from available data on what set of physical security protections would, if implemented for all BPS substations and control centers, assure prevention or effective mitigation of impacts from recent physical attacks. NERC is also unable to measure the effectiveness or the burden of these measures without identifying first the specific threats or specific risk reduction objectives these controls provide protection against.

Additionally, due to the variability of threats and potential impacts, NERC contends that a focus on only considering physical security protection measures as a means of mitigating the impact of physical attacks on BPS reliability is unnecessarily limited. While minimum requirements for physical security protections may reduce the overall amount of some physical security incidents, establishing a minimum set of uniform protections does not guarantee those protections will prevent outages from sophisticated attacks or equipment by determined bad actors. Other reliability, resiliency, and security measures should be considered for additional operational and planning capability – which could include modifications to existing or new requirements – to assure additional reductions in the potential impacts from physical attacks.

Establishing Minimum Level of Physical Security Protections Conclusions

As noted, requiring a minimum level of protections at all BPS transmission stations and substations and their associated primary control centers necessitates a deeper understanding of the objective of any minimum level of protections, risks the controls should mitigate, and industry resources necessary to meet such minimum requirements. A bright line set of minimum physical security protections, while potentially preventing some forms of attack, does not account for the DBT process nor does it guarantee the protections will safeguard against more sophisticated or coordinated attacks. Effective physical security plans should align with the risks intended to be mitigated. These plans should include responsive or adaptive controls, site-specific attributes, and a viable threat assessment from expert security professionals.

Effective physical security plans include more detail than just protections. As discussed in this report, many physical security controls address a combination of detection, assessment, delay, and response capability. This often means that even a high degree of protective controls are not always intended to completely prevent the occurrence of attacks. The likelihood of some impact becomes more probable the more coordinated or sophisticated the attack as typical deterrence controls become less effective. Any physical security controls that are pursued should be based on many factors including site impact, mean time to recovery, and other organization-specific attributes. These factors should be determined through physical security risk assessments to evaluate and define an appropriate selection of physical security protections. When evaluating the physical security controls for transmission stations, substations, or primary control centers, physical security experts provide technical input on the potential threats, criteria, and solutions. While physical security experts may need to work in concert with other registered entities to identify the electrical impacts of the Facilities, these perspectives are highly important when establishing minimum security controls for all Transmission stations, substations, and their primary control centers. Entities are also encouraged to stay engaged with the E-ISAC and current with posted threat intelligence information and guidance.

Reliability, resiliency, and security measures must be comprehensive in scope, and physical security measures should be weighed against other reliability or resilience measures that cover the same risk. Physical security controls may be an option where registered entities cannot implement other resiliency measures effectively to mitigate the impact of localized outages. While physical security controls may provide some level of assurance against physical attacks from occurring, robust resiliency measures are able to provide long-term adaptability to operations, planning, and security from any type of outage. When outages do occur, invested solutions in response readiness and spare equipment strategies are significant in the reduction of resulting impacts. NERC finds that a combination of reliability, resiliency, and security measures are the most likely to help mitigate the impact of physical attacks on the grid. These combined measures provide increased operational and planning capability as well as improved effectiveness of local network restoration. NERC finds that this more holistic approach will provide greater long-term flexibility and minimize the impacts of physical attacks.

Minimum Reliability, Resiliency, and Security Recommendations

In collaboration with the Regional Entities, there have been many proposed solutions on what constitutes a minimum level of physical security for substations and primary control centers. Further, stakeholders have also shared that BPS elements and distribution substations, if attacked in coordination, constitute an attack vector that can have a significant adverse impact to the BES. Based on the assessment in this report, NERC recommends hosting a Technical Conference to discuss the scope of reliability, resilience, and security measures that are inclusive of a robust, effective, and risk-informed approach to reducing risks.[36] The following issues should be considered in the Technical Conference:

[36] In some instances reliability-initiated projects can eliminate the security risk, dependent on a myriad of factors. Potentially, these transmission projects can even alter the outcome of CIP-014 risk assessments to identify a critical substation. The Technical Conference proposed should better refine the scope and feasibility of such outcomes for all substations regardless of criticality or configuration and focus on the risk reduction.

1. The objective of any minimum level of protections, risks to be mitigated, and industry resources necessary to meet such minimum requirements.

2. Expand the use of planning studies to include coordinated security attacks, identify applicable study criteria, and a corrective action plan to mitigate inadequate performance against such criteria as part of their current TPL-001 long-term planning studies.

3. Enhance Operational Planning Assessments to include loss of assets (transmission or generation) from coordinated attacks.

4. Enhance TP and TO requirements to ensure spare equipment pool strategies are adaptive, in-sync, and provide sufficient wide area coverage.

5. RCs develop and train to readiness scenarios reflecting a physical security incident with TOs, TOPs, GOs, and GOPs.

NERC will use the information learned during the Technical Conference described above to determine the next steps, including potential Reliability Standards modifications. NERC plans to consult with FERC staff on the content, timing, and logistics for holding the technical conference. The technical conference on this issue could be held together with or separate from a technical conference on CIP-014 applicability.