NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale

Project 2023-06 CIP-014 Risk Assessment Refinement
Reliability Standard CIP-014-4 | ~~September 2024~~June 2025

CIP-014-4 – Physical Security

In performing the risk assessment, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Attachment 1. The Standard requires the Transmission Owner to perform a risk assessment, consisting of ~~a~~ transmission ~~analysis,~~analyses to determine which of those Transmission stations and Transmission Substations, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection.

The purpose of Reliability Standard CIP-014 is to 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. To properly identify candidates for such Transmission station(s) and Transmission substation(s), the Transmission Owner shall evaluate the criteria listed in Attachment 1.

Rationale for Requirement R1

In the previous version of CIP-014, the 30-month time frame and the 24-month planned-to-be-in-service date could, if not carefully applied, lead to gaps between models and study horizons. Per the Standard Authorization Request (SAR), CIP-014-4 has consolidated these multiple timelines into one.

~~Performing Risk Assessments~~

Requirement R1 is ~~developed~~revised to ensure that each Transmission Owner establishes a list of applicable Transmission station(s) or Transmission substation(s) in accordance with Attachment 1. Aligning the 36 calendar months look ahead in Requirement R1 with the 36 calendar month risk assessment cycle ensures that system topology of the cases used to assess applicability is consistent with the system topology in the risk assessment models.

Transmission Owners shall review and, if necessary, update the list of applicable Transmission station(s) or Transmission substation(s) per Attachment 1 at least once every 36 calendar months. The list of applicable Transmission station(s) or Transmission substation(s) shall include existing or planned to be in service within 36 calendar months Transmission station(s) and Transmission substation(s). The 36 calendar months cycle for updating the list of applicable Transmission station(s) or Transmission substation(s) per Attachment 1 aligns with the annual cycle for performing Planning Assessments per NERC Standard TPL-001. The 36 calendar months risk assessment study cycle aligns with the 36 calendar months planned-to-be-in-service date. "Planned to be in-service" should be taken to mean all Transmission station(s) and Transmission substation(s) as modeled in the base cases for the Near-Term Transmission Planning Horizon.

Rationale for Requirement R2

~~Each Transmission Owner shall, at a minimum, consider the specifications in Requirement R2 for general applicability to their systems, and whether specifications and thresholds need to be stipulated for each Parts 2.1 and 2.2 in their documented criteria.~~

The distance chosen in requirement R2 is based on guidelines that considered a variety of plausible attack scenarios capable of rendering a substation inoperable.

~~A certain amount of discretion and flexibility is intended to be allowable for each Transmission Owner in their respective proximity criteria to document, establish, and demonstrate from a technical basis that various aspects of proximity for their Transmission station(s) or Transmission substation(s) either are or are not appropriate to consider in their risk assessments.~~

The drafting team choose 1500 feet or 457 meters (the shortest distance, measured substation fence line to substation fence line) in Requirement R2 is based on the study from America's Cyber Defense Agency developed in partnership with the Federal Bureau of Investigation (FBI). The Department of Homeland Security (DHS)-Department of Justice (DOJ) Bomb Threat Stand-Off Card is a quick reference guide providing recommended evacuation and shelter-in-place distances for various types and sizes of Improvised Explosive Devices (IED).[1]

Accurate simulation of the event was deemed a priority of the Drafting Team (DT). The DT felt that ownership of proximate substations, as identified in Requirement R2, was irrelevant to Bulk Electric System (BES) impact.

Rationale for Requirement R3

Per Requirement R3, each Transmission Owner is required to have a risk assessment methodology, ~~but the SDT intends for each TO to have flexibility to define its own methodology,~~ including the criteria by which analytical results will be examined to identify Transmission station(s) or Transmission substation(s) 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 ~~TO~~Transmission Owner is not required to develop its own methodology and is free to use a methodology developed elsewhere, such as in coordination with neighboring ~~TOs or~~ Transmission Owners or Independent System Operators (ISOs).

Rationale for Requirement R3, Part 3.1

~~TOs~~Transmission Owners should ~~have the flexibility to~~ determine the amount of ~~acceptable~~unacceptable load loss~~, acceptable~~ and generation loss~~, or other measurements of system response~~ when determining the impact of an event to the Transmission system. Criteria for measures such as load loss or generation loss should consider the impact to the Interconnection ~~instead of local impacts~~.

Large loss of generation or load due to the evaluated disturbance~~, as well as consequences of isolating faulted equipment,~~ could result in severe System impacts. The documented risk assessment methodology shall include the amount of ~~acceptable~~unacceptable load loss~~, the amount of acceptable~~ and generation

[1] https://www.cisa.gov/resources-tools/resources/dhs-doj-bomb-threat-stand-card

loss, ~~and post-event response resulting~~that could result in instability, uncontrolled separation, or Cascading within an Interconnection. Conditions and thresholds used for determining critical Transmission station(s) or Transmission substation(s), i.e., those that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection, should be part of the documented risk assessment methodology.

It is up to the ~~TO~~Transmission Owner to identify post-event measures that can be used to assess the criticality of a Transmission substation or Transmission substation. Suggested measures are listed below. A ~~TO~~Transmission Owner can decide that one or more of the items are not applicable to their location within the interconnection and if any additional items should be included.

~~These thresholds can be treated as proxies for other conditions such as excessive frequency deviation.~~
The following parameters can be used to evaluate the steady-state and/or dynamic analysis:

- Steady state voltages
- Transient voltage response
- Thermal loading of Facilities
- Relay loadability
- Rotor angle stability
- Frequency exceeding generator limits
- Frequency stability
- Acceptable damping of oscillations
- Cascading line tripping
- Steady-state voltage stability

Rationale for Requirement R3, Part 3.2
The performance of both steady state and dynamics simulations is required for all applicable Transmission station(s) and substation(s). Dynamic simulations are required by the ~~SAR after NERC and FERC determined that~~Standard because exclusively performing steady-state simulations ~~alone~~ are insufficient for determining whether the loss of a Transmission station or Transmission substation could result in instability, uncontrolled separation, or Cascading within an Interconnection.

~~Transmission Owners shall develop documented criteria for the conditions listed in Requirement R3, Part 3.1.1, which includes branch thermal exceedance thresholds, bus voltage exceedance thresholds, load loss thresholds, generation loss thresholds, etc.~~
Rationale for Requirement R3, Part 3.3
~~The DT believes that~~A simulation of a ~~fault is~~Fault provides a reasonable assumption for possible events that could impact a single Transmission station or Transmission substation, and for events that could simultaneously impact multiple Transmission stations or Transmission substations.

Rationale for Requirement R3, Part 3.4

The requirement that simulations shall assume the loss of communications and system protection is consistent with the SAR. ~~It is also consistent~~In accordance with the ~~use of~~SAR, the term "inoperable" ~~in the standard.~~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. Each simulation should also include the removal of all Elements that Protection Systems and other controls are expected to automatically disconnect for the event.

~~**Rationale for Requirement R3, Part 3.4.1**~~

~~The DT believes that the use of delayed or remote clearing times is consistent with the description of a Transmission station or Transmission substation being rendered inoperable by an event that disabled local protection systems.~~

~~**Rationale for Requirement R3, Part 3.4.2**~~

While there are commonly used generic clearing times for remote clearing that are consistent across the industry, actual clearing times can be shorter or longer depending on conditions and design considerations at an individual ~~TO~~Transmission Owner. The difference of a few cycles can have a significant impact on the transient behavior of generating units, therefore, it is required that the risk analysis use actual ~~clearing times~~ or more conservative ~~values~~clearing time.

Rationale for Requirement R4

Joint ownership of Transmission substations and Transmission stations was discussed in the Guidelines and Technical Basis of previous versions of the CIP-014-3 standard, but the needed prescription on this issue was missing from the standard language. Because the CIP-014-4 Risk Assessment Refinement SAR calls for clarification regarding Transmission substations and Transmission stations of differing ownership, this section was ~~moved to its own requirement within~~clarified in Requirement R4.

Rationale for Requirement R5

An objective of the CIP-014-3 Risk Assessment Refinement SAR was to align study periods, frequency of studies and the powerflow models used for the studies. A 36-month periodicity was chosen for the R5 risk assessment to reduce the periodicity options from previous versions of the standard. Additionally, a single study periodicity is more easily aligned with project in-service date considerations and model choices. As called for in Project Scope item 3 of the CIP-014-3 Risk Assessment Refinement SAR, the risk assessment must comply with the methodology developed in R3, so this language was explicitly added to R5.

Transmission Owners shall review and, if necessary, update the list of applicable Transmission station(s) or Transmission substation(s) per Attachment 1 at least once every 36 months. The list of applicable Transmission station(s) or Transmission substation(s) shall include existing or planned to be in service within 36 months Transmission station(s) and Transmission substation(s). The 36-month cycle for updating the list of applicable Transmission station(s) or Transmission substation(s) per Attachment 1 aligns with the annual cycle for performing Planning Assessments per NERC Standard TPL-001. The 36-month risk assessment study cycle aligns with the 36-month planned-to-be-in-service date.

In addition to the performance of the risk assessment using Transmission station(s) and Transmission substation(s) identified in Requirement R1, any proximate Transmission station(s) and Transmission substation(s) identified in Requirement R2 should also be included in the risk assessment. Furthermore, any Transmission station(s) and Transmission substation(s) assessed due to having been identified per Requirement R1 should also be run as part of a proximate Transmission station(s) and Transmission substation(s) group per Requirement R2 if such an identification is made.

Rationale for Requirement R5, Part 5.1

If a Transmission Owner performs a steady state analysis and identifies a Transmission station or substation that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection, then dynamic analysis is not required for that Transmission station or substation. If a Transmission Owner performs a dynamic analysis and identifies a Transmission station or substation that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection, then steady state analysis is not required for that Transmission station or substation.

Rationale for Requirement R5, Part 5.2

The intent of this Requirement is that Transmission Owners do not have to reassess already identified and protected Transmission stations or substations (Requirement R5.3 and Requirements R7 through R10 still apply to those Transmission stations or substations). A new risk assessment will need to be performed if the Transmission owner wishes to determine whether or not a Transmission station or substation can be removed from identification and protection as outlined in Requirement R7.1.

Rationale for Requirement R5, Part 5.3

Identification of Primary Control Centers

: After completing the risk assessment under Requirement R5 and verified under Requirement R6, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation, that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

~~**Requirement R6 through Requirement R10 are Requirement R2 through Requirement R6 in CIP-014-3. The Drafting Team did not make any changes to these Requirements. Therefore, the technical rationales are not provided here.**~~

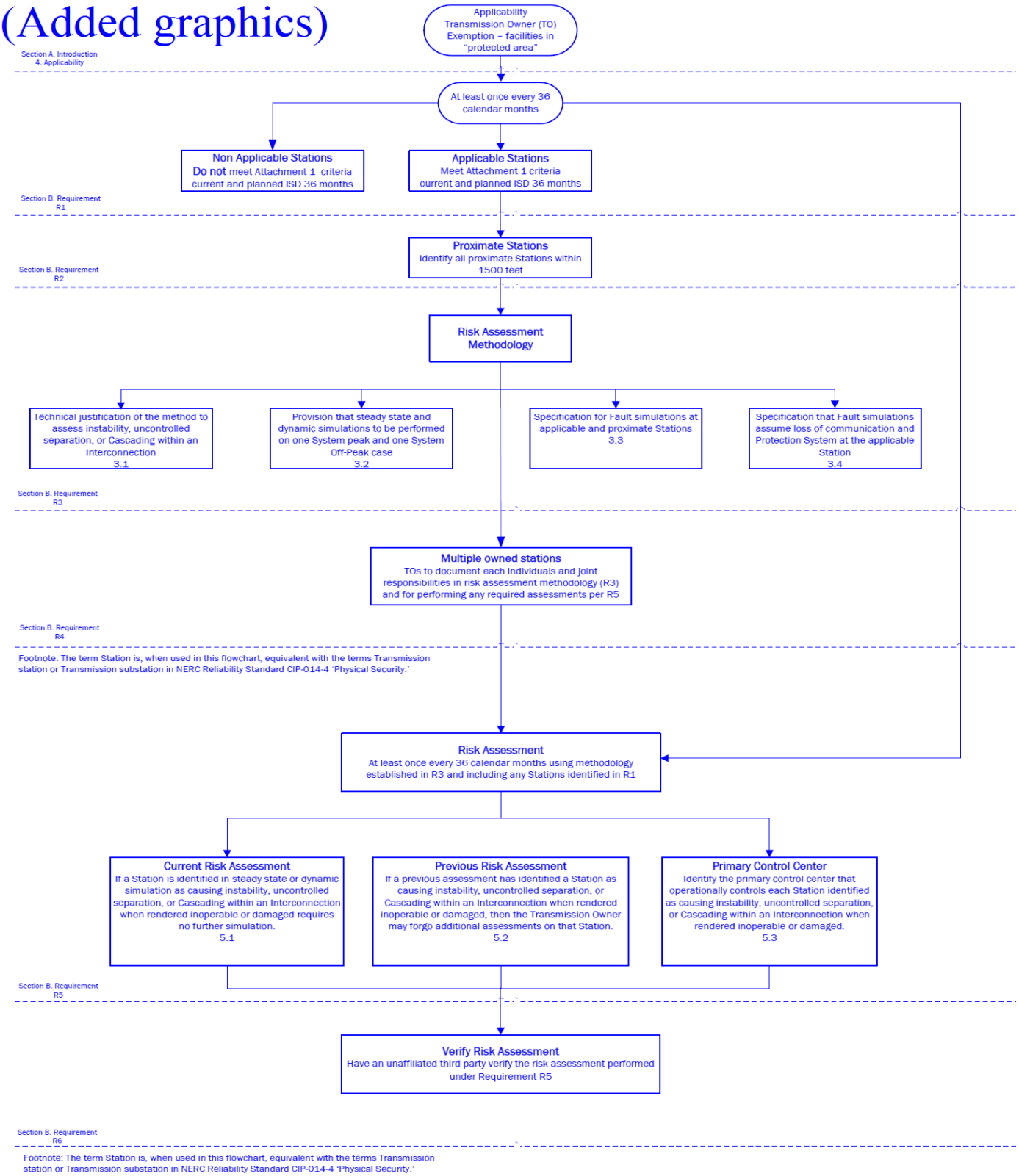
Rationale for Implementation Plan

The Drafting Team has determined that 24 calendar months for the CIP-014-4 implementation plan would allow adequate time for Transmission Owners and Transmission Operators to determine applicability, develop criteria, write or revise methodologies, perform assessments, and procure unaffiliated third parties for risk assessment verification (which some Transmission Owners have performed concurrently with their risk assessment analyses.

CIP-014-4 Flowchart

The flowchart is a concise outline that guides through the steps for completing the risk assessment at least once every 36 calendar months, based on the Applicability in Attachment 1 and Requirements R1-R5.

(Added graphics)



Technical Rationale for Reliability Standard CIP-014-3

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-014-3 standard to preserve any historical references. No modifications have been made.

Requirement R2 (This is Requirement R6 in CIP-014-4)
This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied

concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.

5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3 (This is now Requirement R7 in CIP-014-4)
Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4 (This is now Requirement R8 in CIP-014-4)
This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.

- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5 (This is now Requirement R9 in CIP-014-4)
This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6 (This is now Requirement R10 in CIP-014-4)

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Rationale for Attachment 1

The DT moved the applicability language from CIP-014-3 to Attachment 1 to make the standard easier to read.

The purpose of Reliability Standard CIP~~-014-4~~-014 is to 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. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP~~-014-4 primarily~~-014 first applies to Transmission Owners that own Transmission Facilities that meet the specific ~~applicability~~ criteria in ~~Attachment 1~~Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in ~~Attachment 1~~Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP~~-002-5.1a~~002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in ~~Attachment 1~~Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its 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 Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

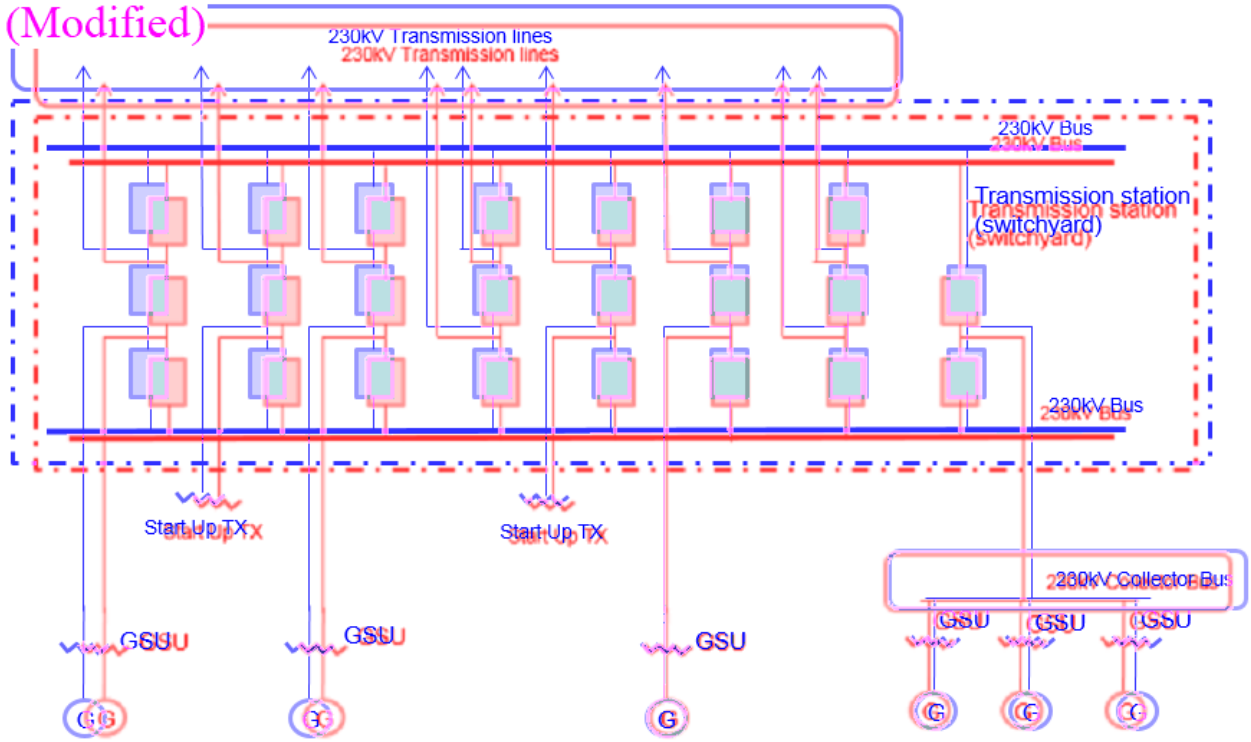
This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement ~~R7~~R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the

Requirement ~~R5~~R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements ~~R8~~R4 through ~~R10. Primary~~R6. In other words, primary control center~~,~~ for purposes of this Standard~~,~~ is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement ~~R5~~R1 and verified in Requirement ~~R6~~R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The ~~DT~~SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause instability, uncontrolled separation, or Cascading within an Interconnection). The SDT determined that ~~continuing to use~~using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-~~002-5.1a~~002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations ~~that~~ must be included in the risk assessment in Requirement ~~R5~~R1 of CIP-~~014-4~~014. Additionally, the ~~DT~~SDT concluded that using ~~CIP002-5.1a~~the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-~~002-5.1a~~002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all 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. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the ~~DT~~SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using ~~Attachment 1, criteria 1~~Applicability Section 4.1.1.1 and ~~2~~4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement ~~R5~~R1

risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in ~~Attachment 1, criteria 2~~Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement ~~R5~~R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



~~Figure from CIP-014-3 Guidelines and Technical Basis~~

Also, the ~~DT~~SDT uses the phrase "Transmission ~~station(s)~~stations or Transmission ~~substation(s)~~substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e.~~,~~ fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the ~~DT~~SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

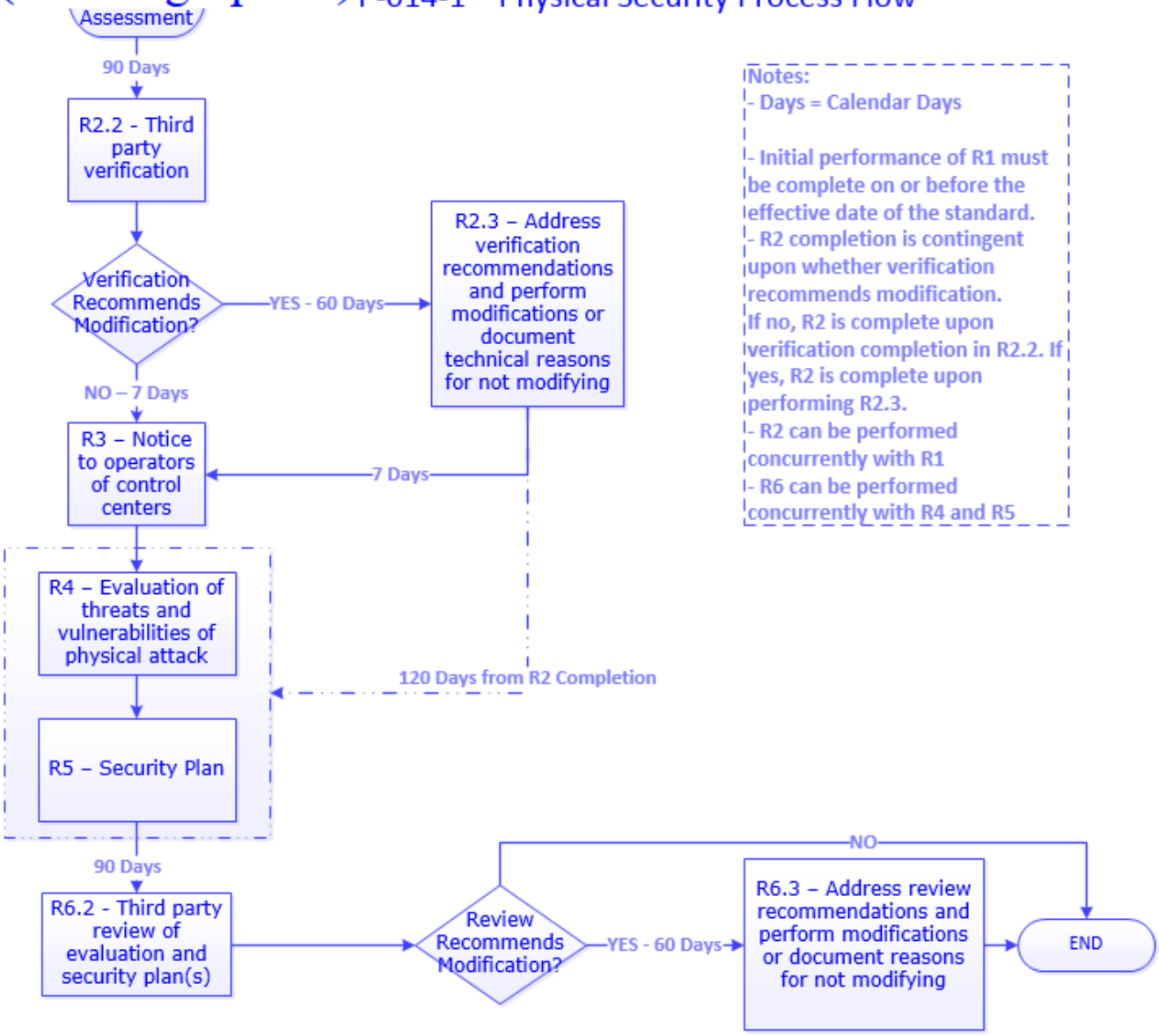
On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate

responsibilities under CIP-014 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014 standard.

Timeline

(Added graphics) P-014-1 – Physical Security Process Flow



Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1 (This is for the old Requirement R1 in CIP-014-3):
This requirement meets the FERC directive from paragraph 6 of its March 7, 2014 order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through instability, uncontrolled separation, or cascading failures. The requirement is not intended to bring within the scope of the standard a Transmission station or Transmission substation unless the applicable Transmission Owner determines through technical studies and analyses based on objective analysis, technical expertise, operating experience and experienced judgment that the loss of such facility would have a critical impact on the operation of the Interconnection in the event the asset is rendered inoperable or damaged. In the November 20, 2014 Order, FERC reiterated that "only an instability that has a "critical impact on the operation of the interconnection" warrants finding that the facility causing the instability is critical under Requirement R1." The Transmission Owner may determine the criteria for critical impact by considering, among other criteria, any of the following:

- Criteria or methodology used by Transmission Planners or Planning Coordinators in TPL-001-4, Requirement R6
- NERC EOP-004-2 reporting criteria
- Area or magnitude of potential impact

Requirement R1 also meets the FERC directive for periodic reevaluation of the risk assessment by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2 (This is now Requirement R6 in CIP-014-4):
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3 (This is now Requirement R7 in CIP-014-4):
Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4 (This is now Requirement R8 in CIP-014-4):
This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation,

provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5 (This is now Requirement R9 in CIP-014-4):
This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6 (This is now Requirement R10 in CIP-014-4):
This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.