UNITED STATES OF AMERICA

BEFORE THE

FEDERAL ENERGY REGULATORY COMMISSION

Physical Security Reliability Standard	**)**	**Docket No. RM14-15-000**

JOINT COMMENTS OF THE EDISON ELECTRIC INSTITUTE, THE ELECTRIC POWER SUPPLY ASSOCIATION, AND THE ELECTRICITY CONSUMERS RESOURCE COUNCIL

The Edison Electric Institute ("EEI"), the Electric Power Supply Association ("EPSA") and the Electricity Consumers Resource Council ("ELCON") (collectively referred to as "the Associations") hereby respectfully submit these Comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("Commission" or "FERC") on July 17, 2014, in the above-referenced docket.[1] The NOPR proposes to approve proposed Reliability Standard CIP-014-1, submitted by the North American Electric Reliability Corporation ("NERC"), the purpose of which is to enhance the physical security measures for the most critical Bulk-Power System ("BPS") facilities. The proposed Standard was developed in response to the Order Directing Filing of Standards issued by the Commission on March 7, 2014.[2] The Associations urge the Commission to approve CIP-014-1 and support the petition filed by NERC in this docket. The NERC petition clearly demonstrates that the proposed standard should be approved by the Commission.

---

[1] *Physical Security Reliability Standard,* RM14-15-000, 148 FERC ¶ 61,040 (2014) ("the NOPR").

[2] *Order Directing Filing of Standards,* RD14-6-000, 146 FERC ¶ 61,166 (2014) ("March 7 Order").

EEI is the association of the nation's shareholder-owned electric utilities and its affiliates world-wide. Its members own or operate approximately 70% of the electric industry assets in this country. In addition, its members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to mandatory Reliability Standards developed and enforced by NERC. It is expected that EEI member companies own the majority of the facilities that will be subject to CIP-014-1.

EPSA is the national trade association representing the competitive power industry. EPSA's members include 15 companies, along with numerous supporting members and state and regional partners that represent the competitive power industry in every region of the country. EPSA's members have significant financial investments in electric generation and electricity marketing operations across the country and therefore support the development of state and federal legislative and regulatory policies that encourage competitive wholesale markets for electricity.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and consumer power in the footprints of all organized markets and other regions throughout the United States.

Members of the Associations are subject to mandatory BPS reliability standards and will be subject to the proposed reliability standard at issue in this NOPR.

I. In Considering the Broader Strategic Issues, the Commission Should Recognize the Importance of Balancing Confidentiality With Coordination and Communication.

The nature of critical infrastructure protection, both cyber and physical security, demands that strategies, plans, tactics, and processes and procedures all take place confidentially. In addition, critical infrastructure protection, especially for the size and complexity of the electric system in this country, requires sophisticated efforts for coordinating and communicating between and among asset owners, law enforcement, and security agencies at all federal, state, and local levels. These two principles require a very careful balancing and form the foundation for the Associations' comments in this docket.

II. The Associations Strongly Support the Commission Proposal to Approve CIP-014-1 as Proposed by NERC.

The Associations strongly support the Commission's proposal to approve proposed standard CIP-014-1. The proposed standard meets the requirements of the March 7 Order and was approved with a strong industry consensus in the ballot body. It represents a reasonable and measured approach to the potential physical security risks to the nation's most critical substations and control centers. The Associations also strongly believe that the proposed standard does not require further modification and that the Commission should withdraw its proposed directives.

The issues around cyber security and physical security continue to rapidly evolve and therefore deserve continued observation and analysis as a strategic matter. The Associations therefore recommend that the Commission engage the electric industry in two years after initial implementation of CIP-014-1 and seek to better understand any opportunities that may exist to

improve upon the focus of the standard. This approach offers an equally effective and efficient alternative to the proposals made in the NOPR that seek to have NERC consider modifications to CIP-014-1. Two years offers a sufficient base of experience that could inform a strategic review of CIP-014-1 by the Commission, including consideration of various implementation issues.

In approving CIP-014-1, the Commission provides necessary flexibility to companies across the country to address critical transmission physical security matters. Company size, extent of transmission asset ownership, transmission configuration, physical location and design of facilities, presence of organized wholesale markets, and prior patterns of theft, vandalism, and other security-related activities, all influence analyses and decisions regarding critical asset identification and risk threat assessments. In addition, the Associations understand that many companies have strong working relationships with field offices of the Department of Homeland Security, and various state and local law enforcement and security agencies. These relationships may influence and facilitate compliance with the proposed standard.

A. The Commission Should Withdraw the Proposed Directive to Allow FERC and Other Government Agencies to Add or Subtract Facilities.

1. The Commission Lacks Authority to Undertake Its Proposed Role under the Standard.

The March 7 order asked that the standard "…include a procedure for the verifying entity, *as well as the Commission*, to add or remove facilities from an owner's or operator's list of critical facilities." (March 7 Order at P 11) (emphasis added). The March 7 Order included no reasoning and explained no basis for this feature. In the NOPR, the Commission states that it proposes to direct NERC to modify CIP-014-1 to include a procedure that would allow "…the Commission and any other appropriate federal or provincial authorities, to add or subtract

facilities from an applicable entity's list of critical facilities." (NOPR at P 23) In support of this proposal, the NOPR states a concern that Registered Entities will face no requirements to add or subtract facilities identified in the course of a compliance and enforcement action. (NOPR at PP. 22-23)

The proposed directive contains problematic legal and practical issues. First, the proposed directive is not compatible with the Commission's authority under Section 215 of the Federal Power Act ("FPA"). Section 215 defines several specific authorities for the Commission, including to: certify one Electric Reliability Organization (215(c)), approve or remand reliability standards proposed by the ERO (215(d)), order the ERO to create or modify a reliability standard (215(d)(5)), resolve conflicts between reliability standards and any other Commission-regulated activity (215(d)(6)), review any penalties associated with violations of Commission-approved reliability standards, including the ability to order compliance with a reliability standard (215(e)(3)), issues regulations for agreements between the ERO and Regional Entities (215(e)(4)), take any actions necessary against the ERO or Regional Entities to ensure compliance with any Commission order affecting the ERO or a Regional Entity (215(e)(5)), and issue orders to determine whether a state action is inconsistent with a reliability standard (215(i)(4)). This statutory scheme does not contemplate a participatory role for the Commission during the risk assessment phase of the compliance process for CIP-014-1. Rather, it gives the Commission robust enforcement power to "order compliance with a reliability standard" after the fact, after notice and an opportunity for hearing. The Commission has not provided a reasoned explanation for pursuing this directive nor addressed its legal authority in the NOPR.

The Commission is an agency of limited powers.[3] Inserting the Commission or any other U.S. federal agency in a mandatory standard is not contemplated by the law.[4] The proposed directive would insert an unprecedented operational role for the Commission in reliability standard compliance that will inevitably conflict with its proper statutory role as a regulator providing statutory oversight, and undertaking compliance and enforcement of its requirements. For example, the right to file a rate is reserved to public utilities under Section 205. The Commission's authority is limited under Section 206 to determining whether a rate meets the statutory standard – whether it is just and reasonable and not unduly discriminatory. Similarly, under Section 215, the Commission cannot take the operational role of a Registered Entity in making the determination of what facilities are covered by the standard. "Registered Entity" is an owner, operator, or user of the Bulk Power System that is included in the NERC Compliance Registry. The Commission is not a Registered Entity. Instead, it is only authorized under the statute to exercise its enforcement authority to determine whether the Registered Entity is in compliance with the standard.

Second, if the Commission were to undertake this decisional and operational role to add or subtract facilities from applicability under the standard, it must also ensure that registered entities have due process rights to seek review of such decisions. It would create an unworkable conflict of interest for the Commission to also review its own operational decisions taken under the statute. Under the FPA, review of a Commission order directing the addition of a facility

[3] *Atlantic City Elec. Co. v. FERC*, 295 F.3d 1, 8 (D.C. Cir. 2002).

[4] The Associations are not commenting on the proposal to revise the standard to grant similar authority to Canadian federal and/or provincial authorities but understand that there are concerns with this proposal as well. The Associations recognize the expertise of the Canadian Electricity Association in this regard and recommend their comments to the Commission.

under R1 would be appealable to the Court of Appeals. Resort to this avenue to protect due process rights would involve costly and time-consuming litigation, and is likely to involve considerable confidentiality concerns. This is not an effective due process remedy for Registered Entities nor is it an effective means for the Commission to ensure compliance with the standard.

Third, in referring to the proposed feature to add or subtract facilities covered under CIP-014, the Commission uses the phrase "any other appropriate federal or provincial authorities" in a way that suggests the Commission may have referred exclusively to Canadian authorities. (NOPR, PP. 17, 23) However, the Associations have concerns that the language could include other U.S. federal agencies. Clearly, if the Commission does not have the authority to play an operational role in the implementation of a reliability standard, it has no authority to insert another federal agency into an operational role – or any other role -- within the standard. Like the Commission, other federal agencies are also limited to the powers granted under their authorizing statutes. As such, there is no basis for another agency to undertake decisional roles that are in effect operational (as discussed above) as well as compliance and enforcement. In addition, as agencies other than the Commission are only authorized and limited by their empowering statutes, they have no authority under Section 215. The Commission can neither authorize another agency to take action under Section 214 nor bind another agency to act only in accordance with the limitations on the Commission's jurisdiction under that section.

For example, should the Commission purport to delegate the power to add or subtract critical facilities under the criteria of the standard to the Department of Defense ("DOD"), would the DOD be prevented from adding a substation that serves what it deems a critical defense

facility such as a military base, without regard to whether that facility meets applicability threshold under the proposed standard (based on the statutory standard), that the substation, if rendered inoperable or damaged could result in "instability, uncontrolled separation or Cascading within an Interconnection"? (CIP-014-1, R1). How would the Commission ensure that the DOD proposed additions (or subtractions) to an entity's list of covered facilities were within the parameters of the proposed standard and in fact complied with the underlying jurisdictional limitations of Section 215? If the DOD did add a substation because it serves a military base and not because analysis shows that it could lead to instability, uncontrolled separation or cascading, what due process remedy would the Registered Entity owner of the substation have to dispute that addition?

While the Commission may wish to seek the expertise of another agency, it cannot delegate authority to another agency to play an operational role under a statute – authority that it does not itself have. The Commission may not delegate an authority that it does not possess. Moreover, as experience shows, utilities work closely with their customers to ensure appropriate security and other reliability measures appropriate to that facility. Nothing precludes a utility from undertaking additional physical security measures to protect substations critical to a particular load such as a defense facility, hospitals or other facilities. However, these actions would not be required under the proposed standard unless the substations meet the criteria in R1, nor would the standard apply to such facilities.[5] Therefore, the Associations request that the Commission clarify that its reference to "appropriate federal or provincial authorities" is not a

[5] *See* March 7 Order at n.5 (recognizing that "owners and operators may protect facilities necessary to serve critical loads "even if the inoperability or damage to those facilities would not result in instability, uncontrolled separation or cascading failures on the Bulk-Power System").

reference to other U.S. federal agencies, but merely recognition of the independent authority of appropriate Canadian authorities as distinct from that of the Commission.

In the NOPR, the Commission raises the concern that corrective action for non-compliance with R1 that would require the applicable entity to correct and repeat the R1 assessment is not a sufficient remedy, stating there is no guarantee that the addition of facilities that the Commission believes should be included would happen in a timely manner, if at all. The Commission has sufficient existing enforcement authority under the FPA to take actions to address concerns raised in the NOPR regarding the sufficiency of decisions made to identify critical facilities under CIP-014-1. This includes the use of traditional enforcement authority under Section 215(e)(3), including audits and investigations, which it has used on several occasions. (NOPR at P 23) Under Section 215(e)(5), the Commission can also direct the ERO or a Regional Entity to "take such action as is necessary … to ensure compliance with a reliability standard." Doing so may trigger the Remedial Action Directive (RAD) process under Section 7 of the CMEP.[6] Specific expedited timelines apply when a RAD is issued, as could be done to add a facility that the Compliance Enforcement Authority determines should be included. There are also strict timelines should the registered entity appeal the issuance of a RAD.[7]

The existing authorities meet the "equally efficient and effective" criterion that the Commission has required when considering proposed standards or potential changes to existing standards.

[6] NERC Rules of Procedure, Compliance Monitoring and Enforcement Program (CMEP), Appendix 4C, Section 7.0, p. 38. See http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4C_CMEP_20130625.pdf

[7] NERC Rules of Procedure, Compliance Monitoring and Enforcement Program (CMEP), Appendix 4C, Attachment 2, at p. 43.

2. The Commission's Proposal Raises Serious Confidentiality Concerns.

The Commission's proposal to have itself included in an operational role in CIP-014-1 raises serious concerns about maintaining the confidentiality of highly-sensitive information about designation and protection of critical facilities. Questions include how the Commission would undertake a review of the Registered Entity's list of facilities under CIP-014-1, while ensuring confidentiality restrictions, including its own Critical Energy Infrastructure Information ("CEII") regulations as well as possible disclosure obligations under the Freedom of Information Act ("FOIA")?[8]

The Commission's CEII regulations are designed to protect information such as that likely to be generated in order to comply with CIP-014-1. CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

1) Relates details about the production, generation, transmission or distribution of energy;

2) Could be useful to a person planning an attack on critical infrastructure;

3) Is exempt from mandatory disclosure under the Freedom of Information Act; and

4) Gives strategic information beyond the location of the critical infrastructure.[9]

[8] 18 C.F.R. §388.113. 5 U.S.C. § 552.

[9] *Id.*

The Commission has recognized concerns about its ability to protect certain CEII-type information from disclosure under FOIA. In a letter to Senator Ron Wyden, [then acting] Chairman LaFleur stated:

> Nonetheless, I agree that it is appropriate to consider whether federal regulation is needed to ensure the risk of physical attacks on our electrical infrastructure is addressed adequately. Thus, I have asked Commission staff to evaluate this issue with NERC under the authority of section 215 of the Federal Power Act. In doing so, we will make every effort to ensure the confidentiality of sensitive security information, recognizing, however, that the Commission is still subject to the Freedom of Information Act even in this area of its authority.
>
> ….
>
> However, in the context of national security concerns, the confidentiality of sensitive security information and the timeliness and certainty of the process, are appropriate concerns. Congress could improve the Commission's and NERC's ability to address the risks related to physical and cyber attacks by enhancing the confidentiality of sensitive security information concerning physical or cyber threats to or vulnerabilities of the bulk power system. A properly-defined exemption from the Freedom of Information Act would be very helpful.[10]

The Department of Energy Inspector General investigated the alleged leak of modeling studies exposing certain grid vulnerabilities and non-public information relating to the investigation of the 2013 attack on the Pacific Gas and Electric Metcalf substation.[11] The findings of the DOE Inspector General Review have raised concerns on the part of owners of critical facilities under CIP-014 as to how any review of such information would be conducted to

[10] Letter from Cheryl A. LaFleur to The Honorable Ron Wyden, February 11, 2014.

[11] *See* Management Alert: Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission ("DOE Inspector General Review"), DOE/IG-0906 at 2 (April 9, 2014)(recommending that FERC seek assistance from appropriate offices in the Department of Energy or other Federal entity "with appropriate original classification authority" to ensure information concerning critical substations is "properly classified and secured"). If the Commission were to add new critical facilities, the Commission would need some analytic basis for doing so contained in reports, analysis, etc. To provide due process, all appropriate personnel from the registered entity should be allowed to review all such data.

ensure its confidentiality. Because of these concerns, review of risk assessments, security plans and other information produced under CIP-014-1 must be conducted on-site.

In addition, the DOE Inspector General Review has raised the concern that information such as that generated during the Metcalf investigation should have been classified. Would the information developed to comply with the standard need to be classified, and if so, would all the personnel at the registered entities involved be able to see the information?

All of these issues invoke potential for unnecessary management and administrative complexity, opportunities for creating duplication and confusion, and potential exposures for mishandling of confidential information.

Therefore, and in light of the Commission's vision that it anticipates taking such actions "only rarely" to identify a critical facility, (NOPR at P 22), the questionable legal authority under which the Commission could act, and the various practical problems associated with implementing such a provision, the Associations recommend that the Commission withdraw its proposal to direct a modification of the standard and instead rely on its existing authority and its specific authorities under Section 215(e)(3) and (5). In addition, the Associations request that the Commission conduct a technical conference in two years to address implementation issues.

B. The Commission Should Recognize That Critical Asset Identification Requires Engineering Judgment.

The Commission proposes to direct NERC to modify the proposed standard to remove the term "widespread" as it appears in the proposed standard in the phrase "widespread instability." (NOPR at P 27) The Associations understand that the Commission has concerns

that the term "widespread" is not formally defined within NERC and that companies' use of such a term may unreasonably reduce the numbers of critical assets identified under the standard. However, this concern is unfounded. The Associations support the language of the standard as proposed by NERC and requests that the Commission not direct changes at this time.

The broad range of decisions needed to inform asset identification requires companies to apply considerable engineering judgments and practices that are qualitative in nature. Such engineering judgments and practices focus a term with broad meaning, whether "widespread instability" or "instability," on those impacts that result in a critical impact to the operation of the bulk power system. The analyses of general phenomenon such as instability could result in identification of stations or substations that would not have a critical impact on the BPS. As an electrical phenomenon, instability may have local impacts or wider impacts, both of which require considerable engineering judgment.[12]

The CIP-014-1 Guideline and Technical Basis discussion for Requirement R1 provides guidance on factors to consider when conducting the risk assessment which aids in achieving an optimum outcome, factors that EEI believes will help sharpen the focus of the analyses. In this manner a Transmission Owner can protect those transmission substations that could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the BPS without expending resources hardening facilities that lack a potential for having a critical BPS impact as a result of damage or destruction.

[12] For example, some personnel may consider that the destruction of a substation may result in generators connected to that substation or nearby to become unstable absent normal protective systems. But the purpose of the standard is not to designate as 'critical' every substation to which generators are connected. March 7 Order at P 12 (expecting the number of facilities identified as critical will be "relatively small compared to the number of facilities that comprise the Bulk-Power System").

The use of engineering judgment and practice is already incorporated and practiced within several NERC processes. For example, the NERC defined term Cascading[13] utilizes the word "widespread" to differentiate a local phenomenon with minimal implications for reliable operation from the more serious phenomenon that does impact reliable operation of the BPS. The definition requires the pre-determined area to be defined by studies which represent an obligation on the Transmission Planner to determine the limits based on "sound engineering practices."[14] In addition, this system performance is allowable under and in compliance with the current Commission-approved TPL-004-0.[15] As a process matter, we envision that such judgments are critical elements that inform whether a "critical impact" could occur as the result of the damage of an asset.

Accordingly, the Commission should withdraw its directive to remove the term "widespread" and instead accept the proposed term as written. Alternatively, if the Commission insists on directing NERC to remove the term "widespread" from CIP-014-1, the Associations recommend that the Commission's final order in this docket clarify that deleting the term "widespread" is not intended to bring within the scope of CIP-014-1 a substation or station unless the applicable Transmission Owner determines through technical studies and analyses that include the application of engineering judgment and practice that the loss of such facility would

[13] NERC Glossary of Terms Used in NERC Reliability Standards – July 7, 2014: "The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies"

[14] Facilities Design, Connections and Maintenance Reliability Standards, 121 FERC ¶ 61,296 at P 112 (2007).

[15] TPL-004 Requirement 1 Category D Contingencies: 8. Loss of a substation (one voltage level plus transformers); 9, Loss of a switching station (one voltage level plus transformers); System Limits or Impact: May involve the substantial loss of customer Demand and generation in a *widespread* area or areas. Portions or all of the interconnection systems may or may not achieve a new, stable operating point. (Emphasis supplied).

have a critical impact on the operation of the BES in the event the asset is rendered inoperable or damaged.

III. The Associations Support the Commission Proposal for an Informational Filing by NERC Focusing on Control Centers.

In the NOPR, the Commission proposes to direct NERC to make an informational filing within six months of the effective date of a final rule in this proceeding, seeking to further inform the Commission on the need to develop mandatory requirements that provide physical security for all "High Impact" control centers as defined under CIP-002-5. (NOPR at P 35) The Commission explains a concern that a successful attack on primary or backup control centers of other functional entities --- Reliability Coordinators, Balancing Authorities, and Generator Operators --- could prevent or impair situational awareness, or could allow attackers to distribute misleading and potential harmful data and operating instructions. (NOPR at P 37)

The Commission has already found that the broad range of requirements in the CIP standards will provide reasonable cyber security for the bulk electric system to support reliable BPS operation.[16] In addition, the Associations agree with the characterization made in the NOPR, recognizing NERC statements in its petition that CIP standards already cover physical and cyber security- related risks for primary and backup control centers under CIP-006-5. (NOPR at P 38) Therefore, the potential scenario of a successful physical attack on primary or backup control centers not otherwise covered by CIP-014-1 represents an extremely unlikely event contingency. The Associations disagree that a need exists to seek comparability between

[16] Order No. 791, 145 FERC ¶ 61,160 (2013); *Order on Clarification and Rehearing*, Order No. 791-A, 146 FERC ¶ 61, 188 2014).

CIP-006 and CIP-014-1 (NOPR at P 39) – protecting two different types of assets, in two different ways. A NERC informational filing will provide a more granular mapping of the strategic considerations embedded in the CIP standards, including CIP-014-1, as well as consideration of the issues relating to control centers not covered by CIP-014-1. Rather than elaborating on these issues in public comments because of potential sensitivities regarding confidentiality, the Associations recommend that the Commission direct NERC, in coordination with the Associations, to submit this informational filing as CEII.

IV. Associations Offer Brief Comments on Generators.

The Commission seeks comments on the potential reliability impact of excluding generator-owned or operated substations, and its proposal to approve R1, the requirement for transmission analysis of substations that connect generating stations through step-up transformers. (NOPR at PP 45, 51) The Associations support the standard and its associated exclusions and attach the CIP-014-1 Guidelines and Technical Basis as support for their position. As stated in the technical basis document: "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 Applicability Section 4.1.1.1 and 4.1.1.2."[17] The Applicability Section 4.1.1.1 and 4.1.1.2 were both approved by the Commission in CIP-002-5. Per Applicability Section 4.1.1, these sections apply to Transmission stations or substations – Section 4.1.1.1 applies to Transmission stations

[17] See Appendix 1 attached to these comments, pp. 28-30.

or substations operated at 500 kV or higher, and Section 4.1.1.2 applies to Transmission stations or substations operated between 200 kV and 400 kV. Therefore, all generators interconnected to applicable Transmission stations or substations will be included in the transmission analysis. As stated in the Guidelines and Technical Basis "the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations." While not expressly included in the Standard's Applicability section, those generating facilities which would have a significant reliability impact on the BPS would be included in the transmission analysis and therefore it is not necessary to revise the Applicability section to include generator owned or operated substations.[18]

V. The Associations Request a Technical Conference on Infrastructure Resiliency.

The Commission seeks comment on a proposal to direct NERC to submit an informational filing that addresses BPS resiliency when confronted with the loss of critical facilities. (NOPR at P 57) The Associations agree that the electric industry needs to continuously review its broad portfolio of resiliency strategies and tactics. While a NERC informational filing may offer some limited value, a technical conference would be more effective.

While the term "resiliency" has no formal definition within NERC, the electric industry has a long history of ensuring the resiliency of the networks, and the production and delivery facilities necessary to operate those networks. Resiliency efforts are reflected in a broad range of

[18]The Associations request that the Commission confirm the exemption on page 2 in the Applicability section that nuclear facilities are not covered by the standard, whether or not the Commission was to determine that owned or operated by generators should be included under the standard.

programs and activities, including coordination with federal, state, and local emergency management agencies and law enforcement for addressing natural disasters, operating emergencies, and vandalism and theft. Many companies have long histories of resiliency efforts reflected in asset management and inventory programs geared to "storm season" risks, which include service restoration planning for conditions where distribution systems require significant repair. More recently, resiliency efforts have focused on high voltage power transformers, including development of the Spare Transformer Equipment Program sponsored by EEI. In broader terms, resiliency may also include more traditional resource adequacy issues, some of which involve markets and tariffs, and others for state utility regulatory review and approval.

All of these various initiatives rest on the basic network design principles of defense-in-depth through multiple redundancies and, ultimately, that generating stations and transmission lines will shut down to protect themselves under various threatening conditions. Ranging from hurricanes and ice storms, to anomalies or "faults" on power lines, system planning and operating technical experts over many decades of experience have evolved planning and operations for system resiliency.

Since the Metcalf event in 2013, the electric industry has sharpened its focus on potential risks involving physical security. The Electricity Sub-sector Coordinating Council has reorganized as a CEO-level group that engages the federal government at a high level to understand the issues, share information, and identify actions that companies can take to strengthen various asset protection programs and activities. The Commission now has under

consideration a mandatory NERC standard, CIP-014-1, which, if approved, will further enhance asset protection programs.

Resiliency also rests on the understanding that providing absolute protection against all perceived threats and vulnerabilities can quickly become a costly initiative. Companies must strike a balance, weighing the various risks and related mitigation costs for each and every potential risk. To the extent that the Commission has interest in additional considerations of the issues, the Associations recommend that other federal and state interests become more involved in the discussions, including state utility regulatory commissions.

VI. The Associations Recommend that the Commission Revise The Cost Estimates for OMB Review.

The Associations consider it very important to understand the order of magnitude cost burden associated with CIP-014-1 implementation. Therefore, the Commission should work to understand with some confidence and communicate to OMB a reasonable and well-reasoned cost estimate. Performing the studies and analyses for CIP-014-1 may not be an 'off the shelf' exercise for all companies, especially considering various multi-contingency scenarios.

Developing a security plan under CIP-014-1 will cost far more than $19,000/company. The Associations' members intend to devote the financial and staff resources needed to fully comply with the proposed standard.[19] However, the Associations believe that the Commission should include a more realistic estimate of the costs to comply with the proposed standard because of the influence that the Commission's assessment may have on the judgment of state

[19] Associations understand that one medium-sized investor-owned utility anticipates that third-party contractor support will cost approximately $270,000 for conducting transmission studies under R1, third-party verification under R2, analyses of threats under R4, and support for security plan development under R5.

utility commissions or other regulatory authorities determining the prudence of costs incurred to comply with the proposed standard. Moreover, the Commission's assessment appears to not include the implementation of the actual security measures included in the Registered Entity's security plan for a particular facility covered under the standard.

VII. The Commission Should Explicitly Address Confidentiality Issues in the Final Order.

As noted throughout these comments, the Commission needs to balance the critical importance of confidentiality with the need for various kinds of communication and coordination that needs to take place under CIP-014-1. The Commission should state in its final order in this docket that any data produced or collected by a Regional Transmission Organization (RTO) in accordance with or part of one of the requirements under CIP-014-1 is protected and not available to the market monitor. The Associations have concerns that parties could interpret existing market monitor agreements and RTO tariffs, some of which refer to "all" data, to require RTOs to provide this sensitive information to their market monitors.[20] Identification of critical assets is not within the scope of the responsibility of market monitors and there is potential harm in sharing this information in this context. Therefore, the Commission should explicitly state in

[20] For example, the PJM Market Monitoring Plan, the PJM Market Monitoring Unit primarily relies on data and information gathered in the normal course of business by PJM including "any other information that is generated by, provided to, or in possession of PJM." PJM Tariff, Attachment M, PJM Market Monitoring Plan, Section V.A. Similarly, the MISO IMM "shall have access to data and other information gathered or generated by the Transmission Provider in the course of its operations . . . . This data and information shall include, but not be limited to . . . l. Other information required to be provided to the Transmission Provider under . . . . Applicable Reliability Standard requirements, or government agency orders." MISO Tariff, Module D, Section 54.1. *See also id*. at Section 54.2.1 (IMM may request additional data). The sensitivity of identification of critical substations goes beyond that covered by normal confidentiality provisions. *See* DOE Inspector General Review, *supra* n.11. *See also MISO Breach Latest in Hackers' Effort to Reach Power Grid*, Bloomberg (July 3, 2014), located at http://www.bloomberg.com/news/2014-07-03/miso-breach-latest-in-hackers-effort-to-reach-power-grid.html.

its Final Rule.[21] To the extent that an RTO's tariff could be so interpreted, we request that the Commission require all such RTOs amend their tariffs through Section 205 or Section 206 filings.

In addition, the Commission refers to the NERC petition in this docket on the expectation that NERC will "monitor and assess" the implementation of CIP-014-1, including "defining characteristics" of critical assets, scope of security plans, implementation timelines, and "industry progress" in implementing the standard. (NOPR P 56) Here again, the Associations urge the Commission to hold to the need for maintaining confidentiality of strategic data and information regarding critical facilities. While the Commission must have confidence that the jurisdictional companies are performing under the standard, there is also an equal need to recognize that information of any type offers an opportunity for compromising performance. The Associations look forward to participating in a careful consideration of appropriate communications tools that will inform the Commission on activities taking place under CIP-014-1, while ensuring that data and information are protected.

VIII. Conclusion

For the reasons set forth in these comments, the Associations respectfully request that the Commission approve the proposed standard CIP-014-1 without modification. In addition, the Associations request that the Commission convene a technical conference on the broad topic of resiliency.

[21] At a minimum, if such data were to be collected by a market monitor, we believe that the market monitor would first have to make a filing with the Commission explaining the need for acquiring such data and how the market monitor will protect the information from disclosure. Transmission owners would receive notice of such filing and file comments with the Commission.

Respectfully submitted;

/s/

EDISON ELECTRIC INSTITUTE
David K. Owens
Executive Vice President, Business Operations

James P. Fama
Vice President, Energy Delivery
David A. Dworzak
Director, Reliability Policy
Barbara A. Hindin
Associate General Counsel
Edison Electric Institute
701 Pennsylvania Ave NW
Washington, D.C. 20004
202-508-5000

ELECTRIC POWER SUPPLY ASSOCATION
Nancy Bagot, Vice President of Regulatory Affairs
Jack Cashin, Director of Regulatory Affairs
1401 New York Ave, 12th Floor
Washington, DC 20005
(202) 628-8200

ELELCTRICITY CONSUMERS RESOURCE COUNCIL
John P. Hughes
Vice President – Technical Affairs
1101 K Street, NW, Suite 7000
Washington, DC 20005
(202) 682-1390

September 8, 2014

Docket No. RM14-15

Joint Association Comments

Appendix 1

NERC CIP-014-1 Guidelines and Technical Basis Document

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.
3. The draft standard was posted, pursuant to a Standards Committee authorized waiver, for a 15-day Formal Comment Period with a 5-day Initial Ballot April 10-24, 2014.

Description of Current Draft

This is the second draft of the proposed Reliability Standard, and it is being posted for final ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
5-day Final Ballot, pursuant to a Standards Committee authorized waiver.	May 1, 2014
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: 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 widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 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 has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

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

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread

instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation 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 widespread 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).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Rationale for Requirement R2:

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.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

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.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement

R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

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.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical

security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. 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.

5.2. Law enforcement contact and coordination information.

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

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

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Rationale for Requirement R5:

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.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- 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.
- 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.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally,

examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Rationale for Requirement R6:

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.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

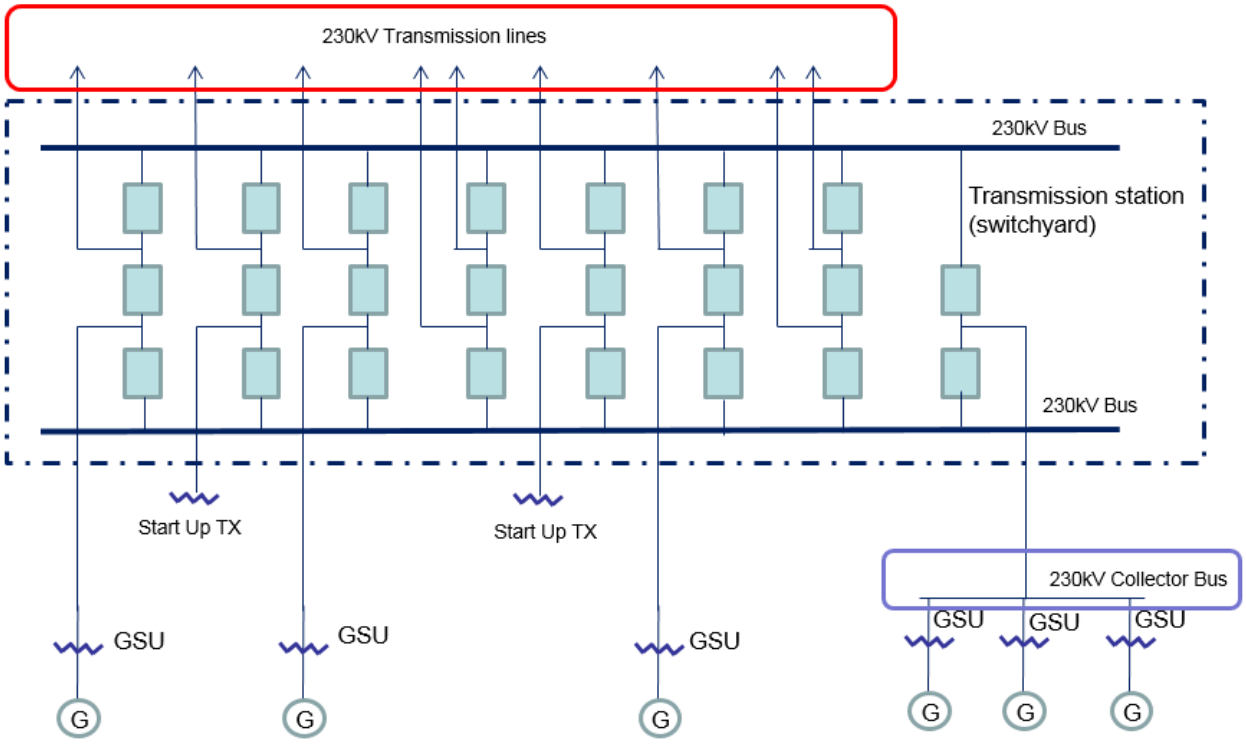
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in 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-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in 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 widespread 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 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 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 R4 through 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 R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The 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 widespread instability, uncontrolled separation, or Cascading within

an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using 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-002-5.1, 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 widespread 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 widespread 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 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 Applicability Section 4.1.1.1 and 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 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 Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement 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.



Also, the SDT uses the phrase "Transmission stations or Transmission 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 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-014-1, 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-014-1 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-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. 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 the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, 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 widespread 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 R2

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 widespread 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

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 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 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 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.*

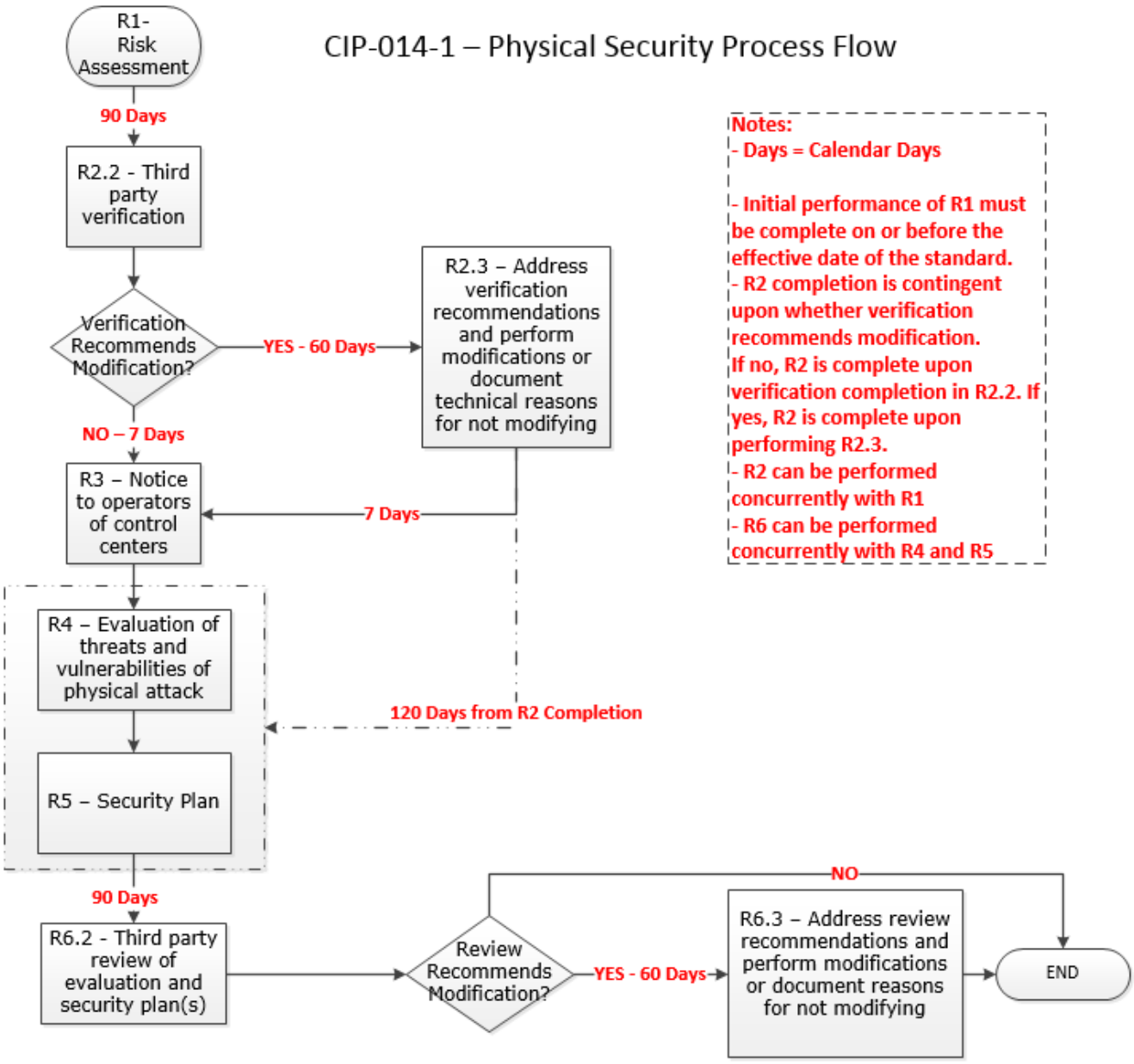
- *A governmental agency with physical security expertise.*

- *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.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5