Consideration of Issues and Directives

Project 2014-04 - Physical Security

~~April 9~~May 1, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~ Transmission ~~Owner~~Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, 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 Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line ~~was appropriate because it has been vetted with stakeholders, and approved by NERC and FERC. The SDT concluded it was~~would provide a ~~technically sound basis to determine~~conservative threshold for defining which

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Transmission ~~Owners should conduct~~stations and Transmission substations must be included in the risk assessment~~.~~ in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities 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; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the ~~methodology~~risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the	*Reliability Standards for Physical Security Measures*, 146	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.	FERC ¶ 61,166 (Mar. 7, 2014).	considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that ~~each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ 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). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history ~~or~~of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		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. Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1)

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
potential physical threats and vulnerabilities they face at the identified critical facilities.		resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4; (2) law enforcement contact and coordination information; (3) a timeline for ~~implementing~~executing the physical security enhancements and modifications specified in the physical security plan; and (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).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with the~~ made available to third party ~~verifier under Requirement R2~~verifiers and reviewers and to protect or ~~the reviewing entity under Requirement R6. These steps will help ensure that lists of critical facilities or other~~exempt sensitive ~~documents remain~~ or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
that is needed to ensure compliance with the Reliability Standards.		confidential~~.~~ information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should 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. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated ~~entity~~third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the ~~verifying entity~~verification shall either verify the Transmission Owner's risk assessment or ~~recommend~~include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		security plan(s) developed under Requirement R5. The reviewing entity must be ~~either~~ (1) 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; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities 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 assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes 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. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
the plan with the Reliability Standards for Commission review.		shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2. - Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 ~~part~~Part 6.2.