NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions
Project 2014-04 Physical Security and Draft Standard CIP-014-1

April 9, 2014

1. Why are NERC and the Standards Committee pursuing a Physical Security Reliability Standard?

On March 7, 2014, the Federal Energy Regulatory Commission (FERC or Commission) issued an order directing NERC to file one or more Reliability Standards addressing physical security of certain critical facilities by June 5, 2014.[1] The Commission stated that the physical security Reliability Standard(s) should require entities to take a least the following three steps: (1) perform a risk assessment of their systems to identify their facilities 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; (2) evaluate the potential threats and vulnerabilities to those identified facilities; and (3) develop and implement a security plan designed to protect against physical attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Commission stated the Reliability standard(s) should also: (i) include a procedure that will ensure confidential treatment of sensitive or confidential information; (ii) include a procedure for a third party to verify the list of identified facilities and review the threat evaluation and security plan(s); and (iii) 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.

In terms of the scope of the standard, FERC stated:

> . . . 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.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

NERC, the NERC Standards Committee (SC), and the Project 2014-04 Physical Security Standard Drafting Team (SDT) have been working diligently, with the assistance of stakeholders through an April 1, 2014, technical conference and SDT meetings, to draft a Reliability Standard that addresses all of the directives issued by FERC in the March 7, 2014, order. Proposed Reliability Standard CIP-014-1 is consistent with the scope of the Commission order and satisfies each directive described above.

NERC does not intend to request an extension of time for filing the proposed Reliability Standard and is committed to meeting the June 5, 2014, filing deadline. The SC and SDT leadership support this decision because they believe the framework in the FERC order is sufficiently clear to develop and file a Reliability Standard by the June 5, 2014, deadline.

2. Why does the proposed Reliability Standard's applicability section start with Transmission stations and Transmission substations identified under the medium impact criteria in CIP-002-5.1?

The SDT developed a technical guidance document appended to the end of CIP-014-1 that explains the applicability section and the requirements of the Reliability Standard in more detail.

In brief, the SDT concluded that FERC's March 7 order is reasonably understood to focus on the most critical Transmission facilities and determined that the CIP-002-5.1 bright line medium impact criteria for Transmission stations and Transmission substations was the appropriate place to start. The CIP-002-5.1 bright line medium impact criteria has been vetted with stakeholders, NERC, and FERC, and provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment under proposed Reliability Standard CIP-014-1. The SDT considered and rejected higher bright line thresholds because the SDT determined that higher bright lines could not be technically justified and may inadvertently exclude Transmission Owners that could have Transmission stations and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

The SDT understands that many of the Transmission Owners that have Transmission stations and Transmission substations that meet CIP-002-5.1's medium impact criteria are unlikely to have a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To that end, if a Transmission Owner's risk assessment does not identify any such Transmission stations or Transmission substations and that risk assessment has been verified by a third party, the Transmission Owner has no further obligations under the proposed Reliability Standard, except to conduct subsequent risk assessments every five years to confirm that it continues to have no such facilities.

The SDT estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In turn, only a small number of Transmission Owners will actually have performance obligations under the entire proposed Reliability Standard. While the applicability section may include additional Transmission Owners subject to Requirements R1 and R2 only, the SDT found that the slightly broader applicability is necessary given the FERC directives, the inability to technically justify a higher bright line, and the importance of being conservative on applicability given the nature of the Reliability Standard's important topic.

The SDT also does not believe more study or time will justify another or higher bright line, given the diversity of Transmission Owners and the highly confidential nature of information related to the applicable Transmission stations and Transmission substations.

3. Why were Generator Operators and Generator Owners not included?

The SDT considered whether to include Generator Operators and Generator Owners in the proposed Reliability Standard and decided not to include them as applicable entities. First, the FERC order does not explicitly mention generation assets, and the order is reasonably understood to focus on the most critical Transmission Facilities. Second, the proposed Reliability Standard accounts for the loss of generation resources. A determination of whether a Transmission station or Transmission substation that meets CIP-002-5.1's medium impact criteria could, if rendered inoperable or damaged, result in widespread instability, uncontrolled separation, or Cascading within an Interconnection must consider the impact of the loss of generation. Specifically, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation. As such it is not necessary to include Generator Operators and Generator Owners to ensure that the impact of loss of generation is considered.

4. Why are only those primary control centers that have operational control of a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2 included in the proposed Reliability Standard? And what does "has operational control" mean?

The FERC order in footnote 6 specifically mentions control centers as a type of critical facility to be subject to the physical security Reliability Standard. Consistent with the order, the SDT found that it is important to include in the proposed Reliability Standard those primary control centers that have operational control over Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Specifically, the SDT concluded that in order to fully protect the Transmission stations and Transmission substations from causing

widespread instability, uncontrolled separation, or Cascading within an Interconnection as a result of a physical attack, it was imperative that these primary control centers be subject to the threat evaluation and development/implementation of physical security plans similar to the Transmission station(s) and Transmission substation(s) they operationally control.

There are two scenarios that the Standard recognizes related to identified primary control centers. In the first scenario, the registered Transmission Owner of the identified and verified Transmission station or Transmission substation is also the entity that operates the primary control center. In scenario two, the registered Transmission Owner is not the same registered entity that operates the primary control center. In this latter instance, the Transmission Operator would be the entity that operates the primary control center that has operational control of the Transmission Owner's identified and verified Transmission station or Transmission substation. Under scenario two, formal notice is required to the Transmission Operator, and that is covered in Requirement R3.

The phrase "has operational control" is specifically used to exclude from the Standard control centers that have no physical control over Transmission stations and Transmission substations, but only have the capability to monitor Transmission stations and Transmission substations, such as is the case with many, if not all, Regional Transmission Organizations and Independent System Operators. In other words, to have a primary control center in the scope of this Reliability Standard, the primary control center must have the ability to take electronic actions that can cause direct physical actions at the identified and verified Transmission station and Transmission substation, such as opening a breaker.

5. Why are unaffiliated third party verifications (of Transmission station and Transmission substation identification under Requirement R1) and unaffiliated third party reviews (of the evaluations under Requirement R4 and the security plans under Requirement R5) required in the proposed Reliability Standard?

The FERC order requires that the risk assessment be verified by an entity other than the owner or operator, and, similarly that the evaluation of threats and physical security plan be reviewed by someone other than the owner or operator. The order used the term "verify" in the context of identification of facilities and the term "review" in the context of physical threat evaluations and security plans. Therefore, the SDT decided to also use those terms in similar contexts in the proposed Reliability Standard.

a. What does unaffiliated mean?

The term unaffiliated means that the selected verifying and reviewing entities cannot be a corporate affiliate (*i.e.,* the verifying or reviewing entity cannot be an entity that corporately controls, is controlled by, or is under common control with, the Transmission Owner or

Transmission Operator). The verifying and reviewing entities also cannot be a division of the Transmission Owner or Transmission Operator (only applicable for the reviewer) that operates as a functional unit.

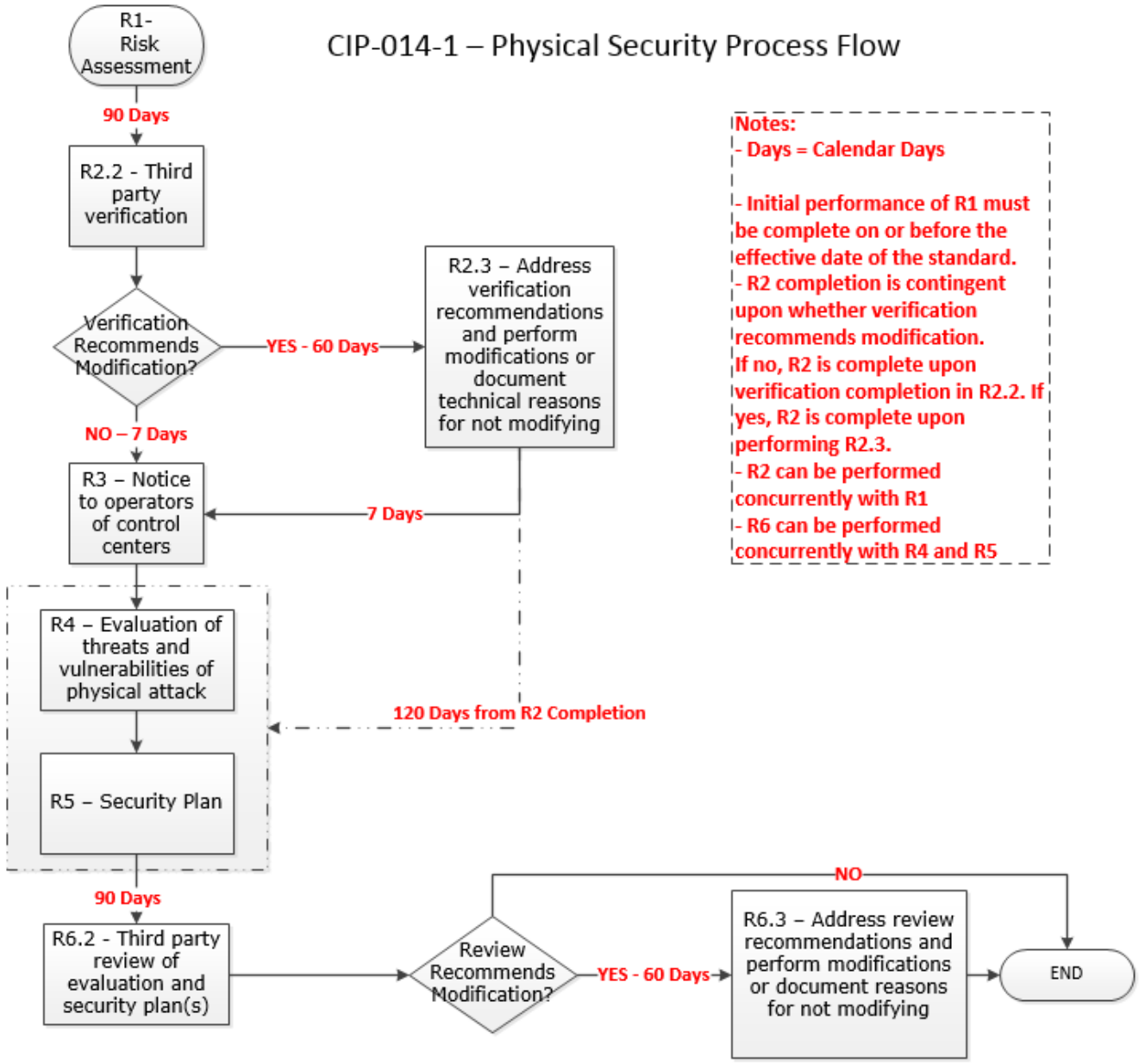
b. Why not "require" unaffiliated Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier of the Requirement R1 risk assessment?

The SDT considered whether to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier and decided against such a requirement. The SDT does not believe it is appropriate to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier. This conclusion is based the following: (i) unless necessary for reliability there should not be a requirement that requires one functional entity to require another functional entity to perform a task; (ii) there are sufficient entities qualified to verify the risk assessment without mandating additional tasks on Reliability Coordinators, Transmission Planners, and Planning Coordinators, and (iii) Requirement R2 provides Transmission Owners the flexibility to consider from many qualified entities.

c. Why is NERC or the Regional Entities not included as a verifier or reviewer?

Similar to reasons provided above for not mandating Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier, the SDT decided against a requirement that would specify NERC or Regional Entities to be the verifier or reviewer. The proposed Reliability Standard, however, does not preclude an entity from requesting NERC or its Regional Entity to be the verifying or reviewing entity under Requirements R2 and R6, respectively.

6. There are several deadlines in the proposed Reliability Standard to complete the risk assessment, third party verification, security plan(s), and third party review of the evaluation of threats and the security plan – can you illustrate this timeline?



7. Why does the proposed Reliability Standard state that the Transmission Owner can work concurrently with the verifier of the risk assessment or reviewer (and the Transmission Operator of the review) of the evaluation of threats and the security plan(s)?

The SDT recognized the value, effectiveness, and efficiency that may result in the Transmission Owner working side-by-side with its verifier, and the Transmission Owner and Transmission Operator, respectively, working side-by-side with its reviewer. Thus, for example, the Transmission Owner may first perform its Requirement R1 risk assessment for identification of Transmission stations and Transmission substations on its own, and then, in a second step, have the verifier conduct its verification of the risk assessment. If more efficient, the Transmission Owner may combine those steps by working side-by-side with the verifying entity to complete the risk assessment and the verification at the same time. It is expected that the selection of this concurrent approach will lessen misunderstandings, and likely be more effective and efficient. This side-by-side approach is equally applicable for conducting the risk assessment and verification under Requirements R1 and R2 and the evaluation of threats, development and implementation of physical security plan(s), and review under Requirements R4 through R6.

8. Given that the TO and TOP will be subject to unaffiliated third party review, does that change how compliance and enforcement will be conducted for this proposed Reliability Standard?

The SDT expects auditors will use their professional judgment to assess the third party reviews and rely on them to avoid duplication of efforts as is permitted by auditing standards. However, some degree of auditor due diligence related to the third party review is necessary to provide a sufficient basis for reliance on the work of others. Documentation regarding the qualification of third parties and the scope and nature of their reviews will help facilitate reliance for compliance auditors. The Notes to Auditor sections of the draft RSAW associated with proposed CIP-014-1 supports the concept of considering the effect of third party verifications and reviews on audit risk and related rigor of compliance procedures.