Unofficial Comment Form
Project 2014-04 Physical Security

Please **DO NOT** use this form for submitting comments. Please use the [electronic form](#) to submit comments on the draft Physical Security Standard Authorization Request (SAR). The electronic comment form must be completed by **8:00 p.m. Eastern on March 28, 2014**.

If you have questions please contact Stephen Crutchfield via email or by telephone at 609-651-9455.

The project page may be accessed by [clicking here](#).

**Background Information**

On March 7, 2014, FERC issued an order directing the ERO to develop a standard to address the physical security of critical facilities on the Bulk-Power System. In the order, FERC stated:

“The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order.”

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.
Questions

1. Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.

[ ] Yes
[ ] No

Comments: Agree generally with the scope. Care must be taken that the requirements developed are consistent with the applicable reliability functions as noted in the SAR. The scope of the standard should be limited to protection against physical attacks. The determination of which physical facilities to protect (identified to be “critical”) should come through a BPS assessment of risk that will need to be defined in the Standard, and depending on how that is done, might involve other types of registered entities or work done under other standards (e.g., CIP or even the GMD Stage 2 effort in which a new TPL Standard is under development, for similar reasons of determining what system risks to address).

Regarding the Applicability, the purpose of this project is develop a standard that will require owners and/or operators of the Bulk Power System, as appropriate, to identify facilities on the Bulk Power System that are critical to the reliable operation of the Bulk Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. Such tasks might require power system impact analyses not unlike the type required for system impact assessments, with a focus on losing all the facilities at a location (e.g. a transmission substation, a large power plant, a right of way, etc.). We do not disagree with the applicable entities as specified in the proposed SAR, but are looking for clarification on how the assessments are obtained, and whether other functional entities might be asked for input from owners/operators. Put another way, depending on the types of impacts the Standard will seek to protect against, entities within the entire Interconnection, or maybe even specific regions within the Interconnection, might need to be included in the Standard.

Can NERC or the SDT provide guidance on whether the loss of generating facilities might have interconnection or area wide impacts that the Standard needs to protect against happening?

To avoid compromising operations as stated in the SAR, we believe that consideration should be given to entities focusing more on the resiliency and the redundancy of the network rather than on additional physical security measures. Attacks may not be able to be prevented, but the consequences of an attack can be mitigated. This is the type of assessment that is best performed using the techniques in the TPL standards.

Furthermore, according to the SAR, the SDT is to develop a standard that addresses risk factors, levels of acceptable security and the implementation of a protection plan. We believe that these elements
can not be standardized as threat assessments are not the same from one entity to another. Consequently, the acceptable levels of safety cannot be identical.

All of these factors lead us to believe that the development of fixed criteria regarding levels of acceptable risk and security cannot be identical from one entity to another. The SDT also has to consider and address the standard with respect to Canadian differences.

2. Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance.

☐ Yes
☐ No

Comments: There are regional differences in Québec. The SDT should not establish predefined criteria for risk assessment since it cannot be the same for different entities. Each entity should have its basis of a threat and security level defined accordingly.

3. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.

☐ Yes
☐ No

Comments: At this time, it is uncertain whether or not there are any jurisdictional issues that need to be considered by the Standard Drafting Team and addressed in the standard. It depends on the proposed requirements as they relate to detection, protection and reporting of potential physical risks to safeguard physical security. In addition, if the standard should involve protection of nuclear power plants, then there are differences in nuclear power plant regulations between the United States and Canada that may require recognition by the proposed standard.

4. Are there any other concerns with this SAR?

☐ Yes
☐ No

Comments: The Standard Drafting Team is urged to not be too prescriptive in the development of these requirements. Operators should be able to conduct a vulnerability assessment and implement any mitigation actions that were deemed appropriate by the entity.
The Standard Drafting team should carefully consider the cost impact that the standard will have on entities to implement and therefore limit the site selection.

Minimum vulnerabilities should be defined to be included in vulnerability assessments.

Critical facilities determination are recommended to be carried out via a TPL standard based assessment.

Timing should be provided for the effective date of standard versus the time required to conduct assessments and implement the mitigation actions identified.

It has to be considered that electrical analysis and physical analysis are related, but are not one in the same. For example, using an electrical criteria, e.g., >3,000MVA, does not take into account that multiple voltages can reside on a single site, within a single footprint and fence. “Substations” is not a stand alone term. The SAR needs to recognize that there is not a total correlation between Cyber Security (CIP-002-5.1) and Physical Security (CIP-014-1). They are related, but different, and may need to use identical and as well as some different criteria. The current proposal for CIP-014 is to use the same criteria as those specifying a Medium Asset in CIP-002-5.1. This may represent an over simplification. Physical Security is different. You do not need access in order to violate physical security. A TPL standards based assessment is a better approach.

The SDT must ensure that the scope of this standard and applicability of facilities subject to the standard is consistent with existing CIP standards.

Furthermore, consider the impact of this standard on the existing standard EOP-004-2 and ensure the coordination with the EOP-004-2 standard.

We believe that the SDT should consider network redundancy in the case of an attack, the potential consequences associated with a physical attack and threats specific to each entity before imposing a standard level of acceptance for all.

The SDT should define how the verification of the risk assessment used by the owner or operator of critical facilities will be completed. The standard should identify the methodology by which critical facilities were identified. Once the methodology is determined, then the SAR should also define the methodology for doing this verification.

The definition of the methodology for review should be applied to the review of all three of the identification of critical facilities, determination of threats and vulnerabilities, and mitigation plans,
and that the standard should clarify whether the mitigation plans also have to be reviewed by a third party.

The SDT should ensure that the new standard does not call for requirements that will impact or impede the normal operational capacity, access for maintenance or restoration, or the safety of people or equipment.

The standard should clearly define the timelines for conducting assessments and implementing the mitigation actions identified with respect to when the standard becomes effective. Timelines for assessment of risk or vulnerabilities in this new standard should coincide with the timelines for which assessment of risk or vulnerabilities for other standards including the CIP and the new GMD Stage 2 project which will be a new TPL standard.