NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Considerations for Transmission Owner (TO) Control Centers (TOCC) with Capability to Perform Transmission Operator (TOP) Obligations

Project 2016-02 Modifications to CIP Standards
March 14, 2017

Introduction

The "TOCC White Paper" provides background and technical considerations for potential approaches to modifying the applicability of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards as they relate to the protection of BES Cyber System(s) at Transmission Owner Control Centers performing the functional obligations of a Transmission Operator. The TOCC White Paper was drafted by the standard drafting team ("SDT") for NERC Project 2016-02 Modifications to CIP Standards (Project 2016-02) for stakeholder consideration and comment. The TOCC White Paper has not been approved or endorsed by NERC. The SDT is using the TOCC White Paper as a standard development tool to collect feedback on the basis for revisions to the CIP standards on this issue, if any.

As outlined in the applicable Standards Authorization Request (SAR), NERC Project 2016-02, addresses the Federal Energy Regulatory Commission (FERC or Commission) Order No. 822 directives and the issues captured in the Version 5 Transition Advisory Group's (V5TAG) *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document). The V5TAG, comprised of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. In the Transfer Document, the V5TAG outlined the issues which it believed required further modification or clarification within the CIP Reliability Standards. The necessary modifications were believed to support effective implementation; critical infrastructure security improvements; and/or consistency in Compliance Monitoring and Enforcement outcomes.

Among other things, the V5TAG Transfer Document proposes that the CIP SDT address the applicability of the CIP Reliability Standards to BES Cyber System(s) for a TO Control Center performing the functional obligations of a TOP. As such, the SAR for Project 2016-02 lists the following issues for the Project 2016-02 SDT to address:

1. The applicability of requirements on a TO's Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the Bulk Electric System (BES);
2. The definition of Control Center; and

3. The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.

To address the issues listed, the SDT identified the following five areas for examination and discussion: (1) the TOCC responsibilities as they relate to TOP functions or tasks within the NERC registration processes; (2) the roles that entity impact analyses and risk assessments play, including the NERC proposed beta criteria; (3) understanding of the phrase "performing functional obligations;" (4) a technical discussion on the capability vs. authority and span of control of BES Cyber System(s) associated with TOCCs; and (5) consideration of potential solutions. Each of these areas is discussed in this TOCC White Paper.

The SDT is seeking stakeholder feedback on its assessment of the TOCC issue area through the associated informal comment form. In particular, the SDT seeks feedback on the potential solutions proposed in this TOCC White Paper as well as any suggestions for alternative solutions.

V5TAG Background

As described in the NERC Project 2016-02 Standards Drafting Team SAR encompassing the V5TAG transfer document issues, there were multiple readings of the language “used to perform the functional obligation of” in CIP-002-5.1a, Attachment 1, criterion 2.12 and recommendations for clarification of:

- The applicability of requirements on a TOCC that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
- The definition of Control Center.
- The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.

The V5TAG suggested that the Project 2016-02 SDT consider the following potential options or recommendations for resolution:

- Provide additional clarity or revisions to CIP-002-5.1a, Attachment 1. Specifically around Transmission Owner Control Centers performing the functional obligations of a Transmission Operator, in particular for entities with small or lower-risk Cyber Asset risks.
- Clarify applicability of requirements on a TOCC that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Currently, CIP-002-5.1a indicates that any Control Center performing the actions noted above is to be considered as having BES Cyber Systems categorized as medium impact, if not already identified as high impact. There is no allowance for a low-risk entity performing TOP functions to identify their assets as containing only low impact BES Cyber Systems.
- Revise the definition of Control Center if additional clarity will improve consistency in implementation, compliance and enforcement, and determination of applicability.

The TOCC whitepaper is an effort to fully inform industry about this issue and the SDT needs feedback from all industry participants on the topics in the associated comment form.

Related Issues Not in Scope of SAR

As described in the Standards Processes Manual, a SAR is the form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions or the benefit of retiring one or more approved Reliability Standards.

Early in the SDT research effort, discussions with stakeholders revealed a potentially significant connection between the TOCC issue and the ERO Registration processes. The SDT explored this path and captured the following information.

In 2014, NERC completed development of a Risk-Based Registration process, which FERC approved in 2015. During the development effort, NERC considered the concept of a registration *lite* for those entities that may perform functional obligations but have less reliability impacts to the BES. These concerns were not specific to a registered function but were entity-dependent having a relationship with the TOCC. The Risk-Based Registration process concluded and determined there was not a defensible position for a registration *lite* concept, but given the remaining concerns, the ERO established NERC-led review panels developed from the Risk-Based Registration process to assess and confirm an impact rating for TOCCs, should the question arise in the future.

The review panel can be utilized for concerns with registration as a TO or TOP if the entity believes the designation it carries to be inappropriate. Entities that may be impacted by a change in a neighboring or fellow registered entity have a chance to participate in the panel process. To be more direct in linkage, if an entity has concerns about applicability of functional performance or tasks – this would not be addressed in a family of standards – but in the tools and programs as defined in the NERC Rules of Procedure (ROP). These are the ordered processes for any type of exception, if you will, from adherence to the standards and requirements.

In discussions with impacted stakeholders, the SDT learned that some TOPs believe they are inappropriately registered as TOPs and, as a result, are disproportionately impacted by the CIP standards. This registration issue is outside the scope of Project 2016-02. The SDT notes, however, that entities may use existing mechanisms to potentially resolve these concerns.

NERC Project 2016-02 Background

On January 21, 2016, the Commission issued Order No. 822, Revised Critical Infrastructure Protection Reliability Standards, approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee (SC) authorized the SAR to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the SDT made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016. The SC accepted the SAR revisions on July 20, 2016.

The purpose of NERC Project 2016-02 is to increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities. To help accomplish this, the SDT will: (1) address the Commission directives contained in Order No. 822, and (2) consider the V5TAG issues identified in the V5TAG Transfer Document.

It is important to note that the V5TAG issues relate to the language developed by the Project 2008-06 Cyber Security Order 706 Standards Drafting Team (706 SDT) as directed in FERC Order No. 706. The NERC Board of Trustees adopted the stakeholder-approved CIP Version 5 standards and FERC approved the standards on January 18, 2006. The Project 2016-02 SDT must consider the V5TAG issues based on the language of FERC Order No. 706 and the intent of the 706 SDT with a subset of the language captured below.

> 280. The Commission has two concerns regarding the misuse of facilities, and clarifies those concerns here. First, Requirement R1.2.1 requires responsible entities to consider control centers and backup control centers as potential critical assets. In determining whether those control centers should be critical assets, we believe that responsible entities should examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks. Responsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System. The Commission recognizes that, when these matters are taken into account, it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset.

FERC reiterated its position on April 19, 2012 in FERC Order No. 761 (the order approving "Version 4 Critical Infrastructure Protection Reliability Standards"):

> 57. The Commission recognizes the diverging views among commenters regarding the protection of control centers and control systems afforded under the Version 4 CIP Reliability Standards. In Order No. 706, we stated that "it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset." The Commission maintains this view. However, as we observed in the NOPR, the percentage of control centers to be identified as Critical Assets under Version 4 is 74 percent, which is an improvement over the number currently identified under Version 3. Therefore, it is reasonable to approve Version 4 because it will ensure that more control centers are identified as Critical Assets than are identified under Version 3. However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the requirements of Order No. 706.

NERC Proposed Beta Criteria

Prior to the SAR, NERC compliance staff participating in the V5TAG recognized that Control Centers covered by the referenced criterion may not all pose the same level of risk to the BES, which is a fundamental aspect of CIP-002-5.1a impact-based categories. To evaluate each Control Center's risk to the BES, NERC compliance staff developed beta criteria to identify Control Centers that contain medium impact BES Cyber Systems and evaluate the entity risk impact with consideration of a low impact category. The beta criteria are more fully described below.

The first beta criterion of the evaluation posed the following question: "Does the Transmission Owner's facility operate at least two geographically separate transmission facilities?" If the answer to this beta criterion was no, the TO's facility would be identified as an asset that contains low impact BES Cyber Systems. If the answer was yes, then the evaluation moved on to the next criterion.

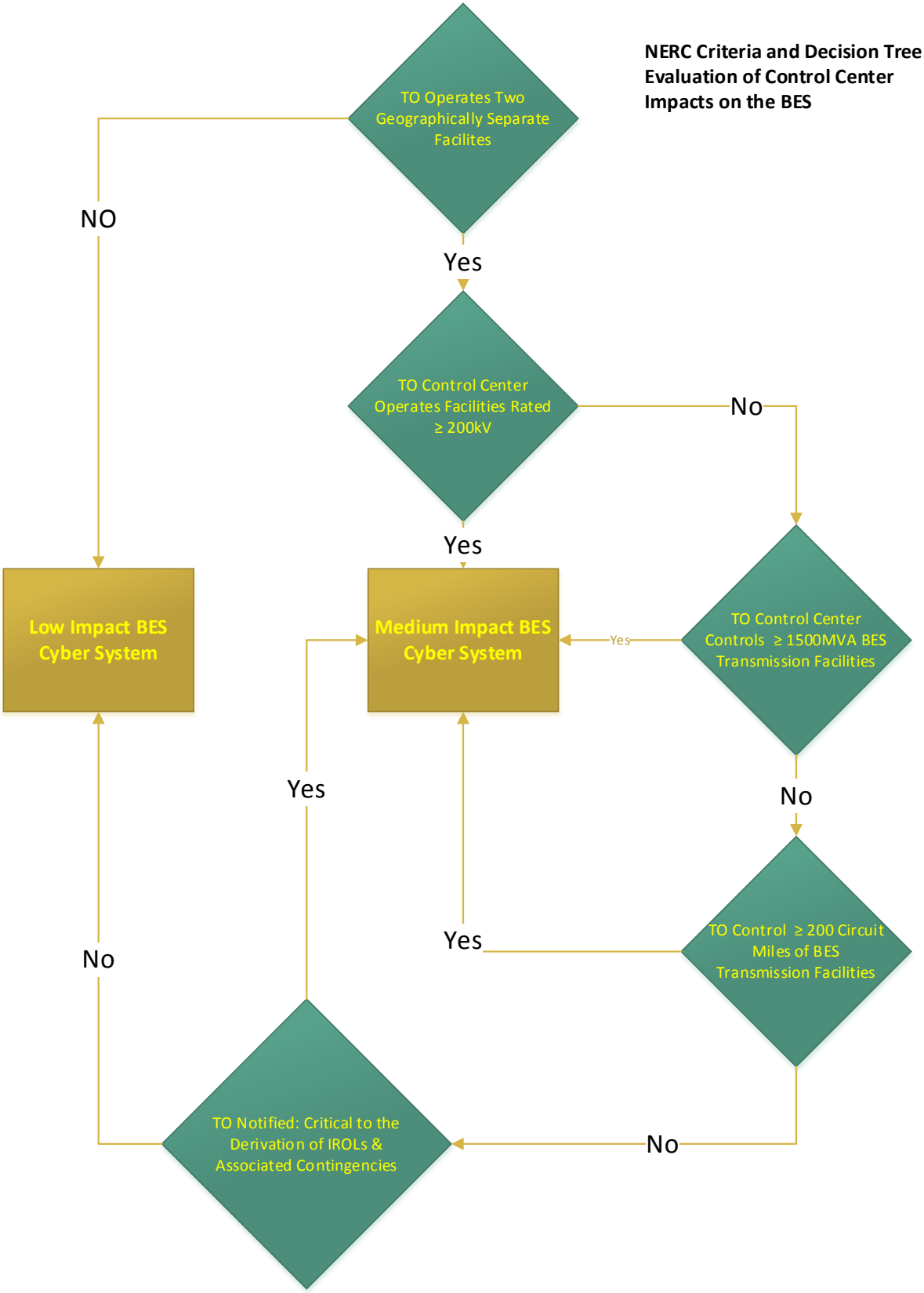
The second beta criterion consisted of the following question: "Do any of the Transmission Facilities operated by the Transmission Owner's Control Centers operate at or greater than 200 kV?" If the answer to this question was yes, then the evaluation resulted in the Control Center being identified as an asset that contained medium impact BES Cyber System(s). If the answer to this question was no then the evaluation proceeded to the next criterion.

The third beta criterion was labeled as the Group 1 criteria and consisted of three distinct questions:

1. "Does the Transmission Owner control 1500 MVA or more of Transmission capacity at BES Transmission Facilities controlled by the Transmission Owner's Control Centers?" It should be noted that this is not Transfer Capability through a Transmission Operator Area. Transmission capacity in this criterion was calculated by adding up the Facility ratings of all the Transmission Owner's BES Transmission Lines and capacitor banks. If the aggregated MVA value was greater than or equal to 1500 MVA, then the Control Center was identified as an asset that contains medium impact BES Cyber System(s). If the answer to this question was no, then the evaluation moved on to the next question.
2. "Does the Transmission Owner control more than 200 miles of Transmission?" This calculation was performed by adding up all of the circuit miles of the Transmission Owner's BES Transmission Facilities. If the answer to this question was yes, then the Control Center was identified as an asset that contained medium impact BES Cyber System(s). If the answer was no then the evaluation moved on to the final question.
3. "Has the Transmission Owner been notified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as having a Facility, controlled by the Transmission Owner's Control Centers that is critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies?" If the answer to this question was yes, then the Control Center was identified as an asset that contained medium impact BES Cyber System(s), if not it was treated as an asset that contains low impact BES Cyber System(s).

The SDT continues to evaluate the beta criteria as an option to pursue. In an effort to clarify the approach as captured, the following flowchart represents the consideration path for execution of the risk assessment.

NERC Criteria and Decision Tree: Evaluation of Control Center Impacts on the BES



Performing Functional Obligations

The SDT delved further into the intent behind the language: "performing the functional obligations of" and identified the following information associated with the creation of this language. The "performing functional obligation of" language was added in CIP-002-4 by the "Project 2008-6 Cyber Security Order Phase II" Standard Drafting Team. The CIP-002-4 Identifying Critical Cyber Assets guideline document references the "functional obligation" language in terms of a "formal delegation" from the registered entity:

http://www.nerc.com/pa/Stand/CIP0024RD/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf

The "functional obligations" language first appears in a draft of CIP-002-4. The draft guidance associated with this first introduction of the language offered the following:

> Part 1.14 designates all control centers and control systems used to perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA) or Transmission Operator (TOP). EOP-008 requires that RCs, BAs and TOPs "ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable." While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets, control systems at other applicable Responsible Entities that are used to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include control systems at Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. Control systems were specifically called out separately from control centers to ensure that Entities fully evaluate those systems used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. These control systems may be located at a data center that is not co-located with the control center itself.

As discussed in summary meeting notes from the aforementioned SDT, the SDT commented on the designation of TOCC's as Critical Assets as follows:

> "As discussed in the Reference Document, this requirement is sourced from EOP-008. Control centers performing these functional obligations are considered important enough to require mandatory backup requirements and warrant designation as Critical Assets."

Given the information discussed above, the relationship to the operations and planning standards vary with different levels of potential impact. To perform functional tasks or obligations, a System Operator must either be certified as a Transmission Operator or Reliability Coordinator (RC) or take direction from a NERC-certified System Operator (Transmission Operator or RC). Maintaining a NERC certification can take significant investment of time and resources, so some System Operators that control BES Transmission Systems do not maintain certification and instead rely on only operating the System when directed by a NERC Certified System Operator. To address the scenario where an individual or entity is 1) performing BES Transmission operations, 2) is not a registered TOP and 3) equipment may have an impact on BES operations, the 706 SDT incorporated the language "used to perform the functional obligations of" to clarify that the equipment used by both NERC-certified System Operators and System Operators operated under the direction of a NERC-certified System Operator had to be protected and fully implement the security objective for protecting equipment used to perform TOP functions. The functional obligations of a TOP are identified in the NERC Rules of Procedure[1], with further examples included in the Functional

[1] http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20161031.pdf

Model and are also summarized in the BES Reliability Operating Services (BROS) in the Guidelines and Technical Basis of CIP-002-5.1a.

1) Capability versus Authority

In terms of CIP-002-5.1a and determination of risk level or impact classification, Attachment 1 criterion 2.12 focuses specifically on those Responsible Entities taking part in or performing both the Transmission Owner and/or the Transmission Operator reliability functions. As stated in the V5TAG Transfer Document, the language "used to perform the functional obligation of," was intended to "capture entities that perform obligations of a specific registered function, whether they are registered for that function or not." The statement inherently accommodates the risk that CIP-002-5.1a Attachment 1 is trying to mitigate. Regardless of how a Responsible Entity is registered, to adequately protect the BES, entities must look at not only the intended use but also the potential misuse of the BES Cyber System(s). If a malicious actor is capable of affecting the BES in a negative manner from a given BES Cyber System, that BES Cyber System needs to be protected accordingly to prevent such actions.

Regarding criterion 2.12, this notion calls into question whether it is appropriate to afford BES Cyber Systems protections based on authority to perform actions (registered functions) or capability to perform actions.

For criterion 2.12 in CIP-002-5.1a Attachment 1, it is clear that the intention is to require application of appropriate protections to BES Cyber Systems operated by Responsible Entities that fulfill TOP reliability functions, regardless of registration. An example of this would be a case where there are two Responsible Entities, one registered as a TO, and the other registered as a TOP. If the entity registered as the TO operates a Control Center and follows directives given by the TOP, the TO is clearly operating on behalf of the TOP. In this case, while the TO only does this when authorized by the TOP, the BES Cyber System(s) associated with the TO's Control Center possess the capability to be used by an unauthorized party to affect the BES, and must be protected as a BES Cyber Asset.

2) Span of Control

The TOP's span of control is not limited to just Transmission Lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, makes it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact Real-time operation for a TOCC.

CIP-002-5.1a, Attachment 1 categorizes BES Cyber Systems into risk based impact levels primarily based on the span of control of the BES Cyber System(s). The premise of this discussion is that the span of control for the TO and TOP functions should be more fully considered to determine whether a risk-basis exists for a low impact categorization for BES Cyber System(s) associated with Control Centers.

Evaluation of Potential Solutions

The SDT evaluated potential solutions (as recommended by V5TAG and others) against the facts and factors uncovered during the SDT research. The associated informal comment form includes questions for stakeholders that are intended to gather additional information and stakeholder positions related to these potential solutions.

1) Propose revisions to CIP-002-5.1a

If the SDT were to take action to respond to the TOCC issue, there are many variations of what may be an appropriate action. The following section proposes potential standard revision options.

a) Propose revisions to CIP-002-5.1a, Attachment 1, Criterion 2.12

The SDT considered the prospect of revising the Attachment 1, criterion 2.12 to add clarity for Responsible Entities. Criterion 2.12 establishes a medium impact level for "Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating (H), above." Under this option, the SDT would propose an impact rating criterion to establish a medium impact rating that would include a lower bound to the criterion. Control Centers with the characteristics listed below would be categorized as assets that contain medium impact BES Cyber System(s), and all others would be identified as low impact BES Cyber System(s). The impact rating criteria would be similar to the NERC proposed beta criteria referenced above. One example of a revised criterion 2.12 is as follows:

Attachment 1: criterion 2.12. Each control center or backup control center not included in the high impact rating (H) above, that is used to operate any of the following:

- Two geographically separate (BES) Transmission Facilities operated at 200 kV or higher
- Transmission Facilities that have an aggregate transmission capacity greater than 1500 MVA
- A Facility that has been identified by its RC, PC, or TP as critical to the derivation of an Interconnection Reliability Operating Limit (IROL) and its associated contingencies
- Facilities operated between 100 and 200 kV that have been identified as part of a permanent flow gate or major transfer path
- BES Transmission Facilities that have a Total Transfer Capability with a neighboring Transmission Operator that is greater than 1500 MVA
- Greater than 200 line miles of Transmission Lines

The SDT assessed the potential for such a revision to the criteria and found trade-offs to the proposal. This option could provide added clarity for Responsible Entities and compliance enforcement personnel in determining the assets that are in and out of scope; however, this option could still cause Control Centers with minimal risk to the BES to be identified as medium impact BES Cyber System(s). This could place significant strain on resources of minimal risk entities and the burden as well as benefit may not be commensurate to the risk of those entities.

There will be implications for both newly registered TOs as well as existing TOs. Updated criteria will trigger an analysis and implementation cycles for entities currently in scope under CIP V5 causing rework depending on what type of criteria might be considered. This is a significant consequence for entities that only recently completed implementation of CIP V5 or will still be in the process of completion of the implementation efforts. The update could likely change the impact classification of affected BES Cyber System(s). While this would be one purpose of the revision, resolution for some would be offset by new issues for others.

While the SDT is considering development of a categorization for Control Centers with a low impact rating, FERC Order No. 706 set an expectation that Control Centers would be identified as "Critical Assets," which correspond to high and medium impact levels in the revised CIP Reliability Standards. Given the overhaul that CIP V5 represents in its expansion of scope to include all BES Cyber Systems, a lower bound for Control Centers may be justifiable.

b) Low Impact Justification Process

Another potential solution is to utilize a justification process that would provide Responsible Entities the opportunity to demonstrate that their Control Center poses a minimal risk/low impact to the BES. As contemplated, a justification process may allow the TO to perform an engineering analysis to demonstrate to the ERO Enterprise that the risk posed by its Transmission Facilities do not warrant protection of the associated BES Cyber System(s) as medium impact. The criteria upon which the ERO would assess the TO's analysis would need to be developed. This justification process could include a review of the TO's analysis by an unaffiliated third party.

This justification process approach could provide the clarity requested by the V5TAG and could also provide Responsible Entities a process to demonstrate its actual impact level as demonstrated by engineering studies. However, this additional process could place additional strain on limited resources for Responsible Entities and Compliance Enforcement Authorities to support the positions that certain Control Centers represent less risk or impact to the Bulk Electric System even in a situation specific to misuse or malicious threat actors.

2) No further action by the SDT

The V5TAG presented a valuable opportunity for NERC, the Regions and industry to consider the CIP V5 language under implementation and consider areas that may benefit from added clarity. However, the SDT evaluation must take into account the breadth and diversity of the entities to which the CIP V5 language applies. The language under evaluation by the SDT relative to the TOCC issues raised by the V5TAG was approved by NERC stakeholders through an open and transparent process. The current state reflects that FERC approved language is in effect and currently no direction to modify the language has been given.

In addition, CIP V5 only became mandatory and enforceable on July 1, 2016. Familiarity with the full implications and effectiveness of the standards is still new and untested.

From research and analysis, the option to take no further action could potentially be based on the following reasons:

- The TOCC situation represents individualized company positions and each entity must be evaluated for risk and impact suggesting a widely applicable standard is not appropriate to represent a norm or majority.
- The currently approved language maintains the intent of the CIP V5 language.
- Revision of the Control Center definition is not needed to resolve this issue and has broader implications that are not limited to this project.
- Standards development should not be utilized to solve potential concern about compliance monitoring or enforcement. Alternative ERO tools exist such as the BES Exception Process and NERC led review panels related to Risk Based Registration Processes should be pursued to resolve entity concerns before revising the approved and implemented standard language. If there is validity or need to open the standards for revision, the SDT is asking for this specific feedback.

The SDT understands that, absent an action not proposed within this TOCC White Paper, a decision to take no further action on the TOCC issue area confirms the existing criteria in CIP-002-5.1a Attachment 1, including criterion 2.12 which identifies all BES Cyber System(s) associated with TOCCs performing the functional obligations of a TOP as medium impact.

Next Steps

The SDT requests industry stakeholders consider the discussion and options detailed above and provide informal comments to the SDT. Input to the comment form questions will help confirm the influential facts and circumstances around this issue and aid the SDT in determining recommended actions.