SERC RELIABILITY CORPORATION

Evaluation | Analysis | Assistance | Operating Experience

2019 CIP Compliance Seminar

This document provides SERC staff responses to questions asked by entities. The information provided herein is intended, on its date of posting, to provide guidance to the industry. Actions based on this information shall have no standing for the purpose of contesting or mitigating any findings of noncompliance by SERC. Compliance depends on a number of factors including the precise language of the Standard, the specific facts and circumstances, and the quality of evidence. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time.

1. A Responsible Entity owns assets, of type *substation*, categorized, using their CIP-002 BES Cyber System Categorization procedure, as containing a low impact BES Cyber System(s).

For Requirement 2 – Attachment 1 Section 2 'Physical Security Controls' of CIP-003-7 'Cyber Security — Security Management Controls', the Responsible Entity plans to implement a documented cyber security physical security controls plan requiring that, the Registered Entity will use at least the following to control physical access to their low impact rated BCS:

- Restricted Key lock on each substation gate
- Fencing or building wall surrounding each substation relay house/yard
- PACS system to control access into relay house (location within the asset)
- Restricted Key lock on each relay house door
- Policy that only those with a need may be provisioned for access
- Policy of conducting periodic reviews (or gap analysis) of physical security controls

CIP-003-7 Attachment 2 states that examples of [acceptable] evidence for Section 2 'Physical Security Controls' is

> "Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access"

Keeping in mind that an asset, of type substation, containing a low-impact rated BES Cyber System(s) requires the lowest tier[1] of risk mitigating physical security controls, it would then seem that an entity could provide as evidence:

- documented cyber security – physical security controls plan
- Evidence of periodic review (or gap analysis) indicating the security controls are in place and working

However, as there is uncertainty as to how far the audit team will drill down, the question becomes: Which, if any, of the following physical security controls, commonly required for physical access security controls at medium-impact rated assets, are required (or at least are expected) to demonstrate compliance with CIP-003-7 R2 – Attachment 1 Section 2 'Physical Security Controls'?

[1] The four tiers being, in order from highest risk mitigation to least risk mitigation, are those associated with CIP- 014-2 "Physical Security", CIP-006-6 "Physical Security of BES Cyber Systems" for high-impact rated BCS, CIP-006-6 "Physical Security of BES Cyber Systems" for medium-impact rated BCS, and finally CIP-003-7 "Security Management Controls".

- List of those personnel provisioned or authorized for access during last 3 years (starting with date of enforcement)
  - Key holders
  - Badge holders
  - Both
- List of the roles that are identified as needing access
- List of the roles that are identified as needing access along with the reason or need for access
- A procedure for identifying 'need for access'
- A documented security review (gap analysis) procedure.
- A procedure to authorize/revoke– unescorted physical access
- A procedure to provision/de-provision an individual for access
- List of those who have accessed the substation or the relay house
- Evidence of implementing procedure to authorize/revoke or provision / de-provision for each person ever having been granted unescorted physical access
- Evidence of testing of restricted key system
- Documented alarm monitoring procedures
- Documented alarm monitoring procedures with ties to the associated incident response plan
- Evidence of testing PACS system other than access granting/denying, for instance testing alarms alerting personnel who can respond, logging of access, and logging of alarms
- An implemented visitor escort program
- Evidence for controls, such as a camera that may be used to monitor, that are not part of the documented plan
- Electronic access controls used to protect the PACS
- Physical access controls used to protect a remote PACS server
- List of those who have physical access to a remote PACS server
- List of those who have electronic access to a PACS Server or Access Control Panel
- PRAs for those granted physical access to BCS or its associated PACS, electronic assess to BCS or its associated PACS

From the perspective of the RSAW Auditor Guidance, it is thought that the list below meets the evidence requirements of the first two line-items of the RSAW's Compliance Assessment Approach for CIP-003-7, R2 (See image capture below), specific to physical security controls.

- documented cyber security – physical security controls plan
- Evidence of periodic review (or gap analysis) indicating the security controls are in place and working

Attachment 1, Section 2

There is uncertainty of what will be evidence sufficient for a 'no finding' during a compliance engagement for the third line item – 'achieved security objective'.

Attachment 1, Section 2

For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has **documented a plan** to control physical access, based on need as determined by the Responsible Entity, to:

1. The asset or the locations of the low impact BES Cyber Systems within the asset; and
2. The Cyber Asset(s), as specified by the Responsible Entity, that provideelectronic access control(s) implemented for Section 3.1, if any.

For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has **implemented its plan** to control physical access.

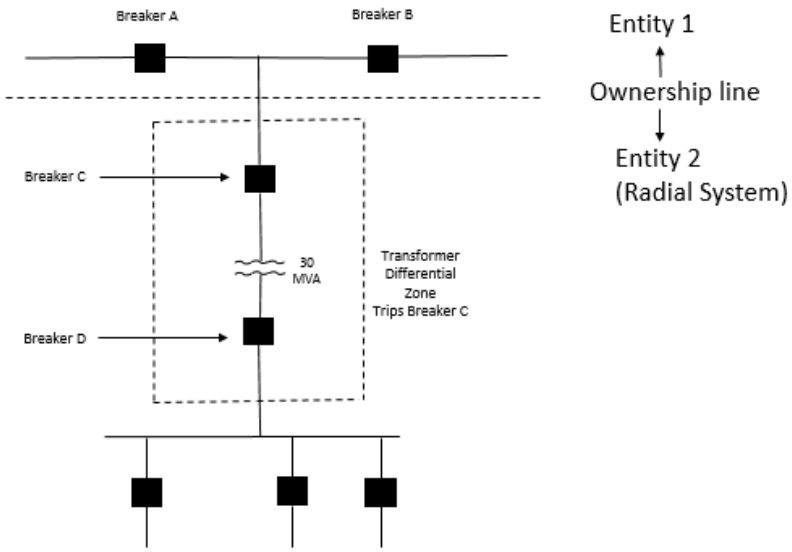
Attachment 1, Section 2

For each asset containing a low impact BES Cyber System, verify that the Responsible Entity has **achieved the security objective** of controlling physical access to:

1. The asset or the locations of the low impact BES Cyber Systems within the asset; and
2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

RESPONSE: SERC cannot prescribe specific controls to meet compliance with the reliability standard in question. Auditors will ask for evidence of the plan to control physical access (including any differences between assets or asset types), validate that the controls were implemented (through examination of evidence, direct observation, and sampling), and evaluate the controls prescribed to identify if they have achieved the security objective (which is as stated in the standard, "control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any").

2. For the following system configuration provided as reference.



As shown, Entity 1 owns all networked facilities as well as the relays protecting those elements. Entity 2 owns a 30 MVA transformer only serving load. Entity 2 has a breaker on the high-side (Breaker C) of the transformer that clears transformer faults. Entity 2's protection scheme does have breaker failure protection that would trip Entity 1 breakers as a means to provide backup protection to the transformer in the event of the failure of a breaker to open. Should Breaker C fail to open upon receiving a trip signal, Breakers A and B would be tripped through a breaker failure scheme after a designed clearing time.

Given that the system owned by Entity 1 contains BES Assets, it appears clear that the protective systems owned by Entity 1 protecting the transmission lines would at a minimum be considered a low

impact BES Cyber System.

Should Entity 2's Breaker Failure relay scheme be considered a Low Impact BES Cyber System just because it trips a low Impact BES Asset?

The breaker failure scheme would appear to be excluded based on the following rationale:

1) With respect to applicability the CIP-002-5.1a Standard states the following.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
   For the scenario described there are not any UFLS or UVLS or Special Protection Systems at the station owned by Entity 2. Therefore it would be dependent solely as to whether or not the Entity 2 owns relays that are BES Cyber Assets which are subject to one or more requirements in a NERC or Regional Reliability Standard. In particular in this case the particular standard would be PRC-005-6.

2) In this case the PRC-005-6 Standard is the only potentially applicable standard that might apply to the breaker failure relay. Therefore consideration is given to the applicability section of the PRC-005-6 standard to determine if the subject breaker failure relay is applicable to the PRC-005-6 standard. The applicability section states the following.

   4.2.1 Protection Systems and Sudden Pressure Relaying that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

   Based on that language for any protective relaying owned by the Entity 2 to be considered as a low impact BES Cyber System it would have to be for the purposes of detecting faults on the BES element, which is not the case here.

   This is further supported by a Supplementary Reference and FAQ dated October 2015 related to PRC-005-6. The drafting team makes the following statement in Section 2.3. where the following language is used.

   2.3 Applicability of New Protection System Maintenance Standards
   The BES purpose is to transfer bulk power. The applicability language has been changed from the original PRC-005:
   "...*affecting the reliability of the Bulk Electric System (BES)…*"

   To the present language:
   "*…that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.).*"
   The drafting team intends that this standard will be consistent with any future definition of the Bulk Electric System. There should be no ambiguity; if the Element is a BES Element, then the Protection System protecting that Element should then be included within this standard. *(Emphasis added)* If there is regional variation to the

definition, then there will be a corresponding regional variation to the Protection Systems that fall under this standard.

Therefore, since the breaker failure scheme for Breaker C is for the purpose of protecting the transformer (which is not a BES Element), it is not a subject to PRC-005 and therefore breaker failure relay is not considered a low impact BES Cyber System. Please confirm the validity of this statement.

RESPONSE: Given the scenario posed, Entity 2 should evaluate the Breaker Failure relay which can initiate a trip on Entity 1's breakers A & B against the BES Cyber Asset definition. This would likely involve coordination with Entity 1 to understand the adverse impact opening breakers A & B would cause. This question has been asked recently in multiple regions and SERC has consulted other regions to ensure a consistent response.

3. Will SERC require a documented justification for inbound or outbound access?

On the SERC website under the "Assistance Catalog /Online Learning/Low Impact" portion of the website referencing CIP-003-6 R2 Initial Performance – Electronic Access Controls, we are trying to determine if SERC has an expectation for Registered Entities to document and provide a business need for electronic inbound and outbound access applied to Low Impact BES Cyber Systems (see attached screenshot)?

CIP-003-6, Requirement 2, Attachment 1, Section 3 doesn't indicate the need for an entity to defend or justify inbound or outbound access deemed required by the entity. The requirement does require an entity to identify necessary inbound and outbound access and to provide access controls to ensure only necessary inbound and outbound access is allowed. The measure supporting inbound/outbound controls in Attachment 2, Section 3 doesn't mention any documentation requirements for the justification of personnel with 'need' for inbound/outbound electronic access. It also doesn't mention personnel justifications for electronic access mentioned in the Guidelines and Technical Basis section related with Attachment 1, Section 3.

Where does it state in the NERC Standard that an entity is required to document and provide evidence at a NERC audit the personnel with a "need" for electronic access applied to Low Impact BES Cyber Systems. (See screenshot from SERC eLearning module below/in FAQ doc.)

Under review. Response to be posted upon receipt.

4. **CIP-002 Low Impact Applicability**
CIP-002-5.1a

As a matter of background, a previous REF question and the reply that SERC provided is referenced below.

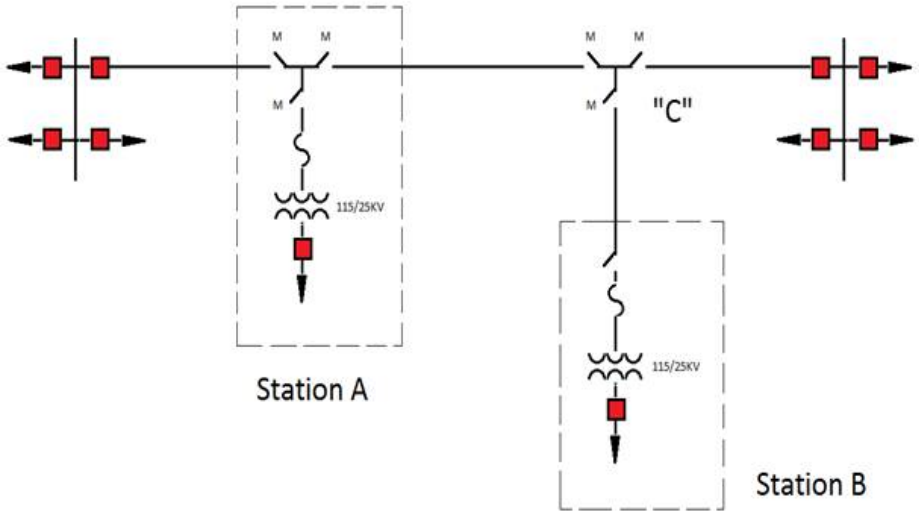
Previous REF Question
R1. States:
Each Responsible Entity shall implement a process that considers each of the following assets for

purposes of parts 1.1 through 1.3:

ii. Transmission stations and substations;

- *The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or 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 (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.*

For the Diagram below:



The switching stations at either end of the line clearly must be considered, but what about Station A? Station B? What about switch "C"?

SERC Responded:

> *Assuming that the horizontal line is a Low Impact BES Element and the four "M" breakers on the horizontal line are BES Elements, Station A will be Low Impact, but the vertical breaker leading down and the items below it are a radial distribution Element and, thus, out of scope for CIP. Station B is radial distribution only; so it is out of scope for CIP*
> *Depending on the configuration details of "C", it may be a BES Element. SERC requires additional information to determine the correct assessment.*
>
> *If there is no remote access to "C," it is not a SCADA point in the EMS, there is no telemetry used by a control center, and it does not qualify as a cyber asset. It is out of scope for CIP.*
>
> *If it can be remotely operated from the control center, it will qualify as a BES Element; and the configuration details will determine if it includes a BES Cyber Asset subject to CIP requirements.*

The response provided by SERC seems to be based only upon whether or not SCADA is used to operate the network switches at Station A and Location C and if they are controlled by SCADA then SERC concluded they are within CIP scope.

It is believed that additional consideration and vetting must be done prior to determining whether or not a Facility is considered to be within the CIP-002 Scope. The following discussion is provided.

1) The standard specifically indicates what assets must be considered. As stated in the CIP-002 Standard (R1).

   R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

   - **i.** Control Centers and backup Control Centers;
   - **ii.** Transmission stations and substations;
   - **iii.** Generation resources;
   - **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
   - **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
   - **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

The only assets that must be considered are those specifically referenced above. In this instance to require consideration, an asset must meet one of the listed criteria as they are neither Control Centers, nor Generation resources, nor do they have SPS that support the BES.

Station A Discussion

In this instance for Station A to require consideration it would be because it met one of the following criteria.

ii. Transmission stations and substations –

The question here is whether or not a distribution station becomes a Transmission station or substation simply because there are network switches within the substation fence. It is felt that most in the utility industry would agree that the facility shown would not be a Transmission station or substation. Although it would be agreed that the network switches may need to be considered since they are BES assets.

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

The network switches could be considered as restoration facilities but additional consideration is required to determine whether or not they are a CIP-002 facility. To require consideration they must be critical to system restoration including Blackstart Resources and Cranking Paths and initial switching requirements. Unless the switches are critical to system restoration there is no basis for them to be included as a CIP-002 location for low impact facilities.

There is approved NERC Guidance that provides clear support for the removal of some BES Facilities from the list of those to be identified as low impact facilities. On page 17 of the approved guidance *Standard Application Guide CIP-002-5.1* dated January 8, 2015 the following is stated (highlighted for emphasis).

2) *Considering BES candidates and determining BES Facilities:* From the list of candidates determined in the previous step, mark those that are out of scope. To do so, differentiate between those candidate Facilities that are BES and those that do not qualify as BES.

a) Remove any Control Centers or Backup Control Centers that do not meet the NERC Glossary definition of Control Center.
b) Remove any Transmission stations and substations that do not meet the BES definition.
   Note: UVLS and UFLS are subject to CIP-002-5.1, and may be located at assets containing Facilities under 100 kV. Registered Entities are encouraged to incorporate provisions into Step 2.b to assure that applicable UVLS and UFLS are identified and that the Cyber Assets/System candidates are evaluated.
c) Remove any Generation resources that do not meet the BES definition.
d) Remove any system restoration systems or facilities that do not meet the NERC Glossary definition of Blackstart Resources or Cranking Paths.
e) Remove any Special Protection Systems that do not support the reliable operation of the BES.
f) Remove any Distribution Provider Protection Systems that do not meet the criteria of Applicability 4.2.1.

One would conclude from using this guidance, that the inline switches at Station A, could be removed if they are not a part of a Blackstart Resource or Cranking Path, as defined in the NERC glossary of terms.

Location C Discussion

With respect to the switches at Location C, the same principles would apply as concluded with Station A. Assuming that the switches are not a part of restoration system or a facility that meets the NERC Glossary definition of BlackStart Resources or Cranking Paths, they would not be in scope.

The only way they would be in scope would be if the switching junction was determined to be a Transmission station or substation.

Review of NERC Approved Guidance

The following excerpts are taken from the NERC approved guidance, *Standard Application Guide CIP-002-5.1* dated January 8, 2015, to illustrate an approved process for determining applicable facilities (Highlights added). It is noted that the in the Guidance, that the non-defined term BES Facility is used to identify impact rated facilities as noted on page 5 of the guidance document.

1. *Preparing the list of BES candidate Facilities*: In an effort to build an initial list of BES candidate assets, the qualifiers within R1 have been removed for this step and those criteria are applied later. From the result in the previous step, document which of the six high level categories in R1 you own. This is your BES candidate list for use in the next step.
   a) Prepare a list of Control Centers and Backup Control Centers
   b) Prepare a list of Transmission stations and substations
   c) Prepare a list of Generation resources
   d) Prepare a list of systems and facilities used for system restoration
   e) Prepare a list of Special Protection Systems
   f) Prepare a list of Protection Systems for Distribution Providers

2. *Considering BES candidates and determining BES Facilities:* From the list of candidates determined in the previous step, mark those that are out of scope. To do so, differentiate between those candidate Facilities that are BES and those that do not qualify as BES.
   a) Remove any Control Centers or Backup Control Centers that do not meet the NERC Glossary definition of Control Center.

b) Remove any Transmission stations and substations that do not meet the BES definition.

Note: UVLS and UFLS are subject to CIP-002-5.1, and may be located at assets containing Facilities under 100 kV. Registered Entities are encouraged to incorporate provisions into Step 2.b to assure that applicable UVLS and UFLS are identified and that the Cyber Assets/System candidates are evaluated.

c) Remove any Generation resources that do not meet the BES definition.

d) Remove any system restoration systems or facilities that do not meet the NERC Glossary definition of Blackstart Resources or Cranking Paths.

e) Remove any Special Protection Systems that do not support the reliable operation of the BES.

f) Remove any Distribution Provider Protection Systems that do not meet the criteria of Applicability 4.2.1.

It appears clear that by applying the steps in the approved guidance, that every BES asset is not required to be considered as a high, medium, or low impact facility.

Summary

It is inappropriate to assume that every BES asset with a Cyber Asset is within scope. In particular every inline switch should not necessarily be in scope just because it is a BES asset. Based on SERC's previous response, it appears that the assumption is that every BES facility with a Cyber Asset must fit into one of the high, medium, or low impact ratings. That seems to conflict with the subset of the facilities listed in the standard.

Questions

1) Is it SERC's position that every BES asset must be an impact-rated facility? If so, please explain how that is consistent with the NERC approved guidance.
   - Based on the previous response SERC may have considered the switches to be breakers since they are referenced as breakers. If so that may have affected the response. The switches are considered to have remotely operated capability.
   - SERC opinion may have been based entirely on the qualifying statement referring to the diagram "*Assuming that the horizontal line is a Low Impact BES Element".* For this example the horizontal line is greater than 100 kV and is a networked facility. The original question was intended to determine if the specified locations were to be considered low impact rather than to assume that they were. If SERC has determined that all BES assets must be included as a low impact categorized asset, please provide the basis for this when NERC approved guidance illustrates facilities can be removed.

   RESPONSE: SERC's position is that Facilities are not impact rated, BES Cyber Systems are. Not every BES Facility will have supporting cyber assets which meet the definition of BES Cyber Assets, which would make such a Facility not "have" high, medium, or low impact BCS. A substation with completely electromechanical protection systems and no RTU or other cyber assets would not have high, medium, or low impact CSs.

2) Should a "distribution station" be considered to fall within the category of "Transmission station and substation" simply because motor operated switches are within the station fence (i.e., Station A), if asked for a list of Transmission stations as the guidance allows for this?

   RESPONSE: All BES Facilities at the asset location should be considered.
   In the CIP-002 Standard Application Guide, page 31, Section Analysis (a copy of the G&TB Section on Attachment 1 Applicability): For *example, for Transmission assets, the substation*

may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems.

"Substation" and "station" are not defined terms, so the G&TB language (restated here in the Standard Application Guide referenced in the question) would indicate that a single location could contain both distribution and Transmission class Facilities, leading to an examination under R1.ii.

3) Is a Switch Junction to be considered to fall within the category of "Transmission station and substation" (Location C)? If so, on what basis?

RESPONSE: If the "Switch Junction" is a location where groups of Transmission Facilities exist, then it should be considered applicable to Rii.

From the CIP-002-5.1a standard, Page 26, Section on Transmission: "The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or 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 (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

4) Is there any basis for removing any of the network switches from CIP scope?

RESPONSE: If they qualify under a BES Exemption, or under the Applicability section, then yes.

Impact

Getting this clarification is important and significant. The current list of locations for low impact facilities that this Entity has identified because of the response given by SERC to the previous REF question is approximately three (3) times larger than it would be if the described facilities were excluded consistent with the NERC approved guidance.

With the upcoming effective dates of additional CIP-003 requirements associated with low impact locations in 2020, and the potential for CIP-013 requirements to be extended to low impact facilities in the future, entities may be significantly burdened beyond the intent of the standard.

Additionally, if other Regions are removing network switches consistent with the NERC guidance but SERC Entities designate them low impact facilities based on SERC REF response, the ongoing Supply Chain Survey may be distorted in this Region compared to other Regions. This might possibly lead NERC to conclude from the results of the Survey, that there are greater risks associated with low impact facilities than actually exist ,simply because of the quantity of locations that will be identified.

5. In a previous SERC Compliance Seminar, SERC stated that it had developed its own version of the NERC CIP Data Request Spreadsheet. Is SERC going to use the new NERC CIP Data Request Spreadsheet version 3.0, or is SERC going to create its own?
If so, will SERC share it with entities outside of an audit?
If not, why not? Entities would like to maintain this spreadsheet on an ongoing basis as an internal control, and in anticipation of upcoming audits.

Under review. Response to be posted upon receipt.

6. What efforts are underway to make the CIP data request spreadsheets consistent across Regions?

Under review. Response to be posted upon receipt.

7. Could SERC explain their method to auditing considering the duplicate questions and amount of effort to complete the RSAWs and evidence spreadsheet?

RESPONSE: Questions on providing policies and procedures to address compliance with the requirements in reference in either the RSAW or the ERT response. The citation should be cited in the RSAW and reference the requirement and any ERT evidence request IDs it is answering.

8. In the 1600 data request, page 5, states that Entities with High or Medium should apply CIP-013 to Low Impact, what would SERC's audit approach be for low impact BES Cyber Systems, PACS, or EACMS as of the effective date of CIP-013?

Under review. Response to be posted upon receipt.

9. MRO has published a Standard Application Guide on physical security for CIP-003 (here). Can SERC discuss or publish something evaluating advantages or disadvantages on maglocks vs cyber locks?

Under review. Response to be posted upon receipt.

10. What is SERC's opinion on the FERC/NERC White Paper on the new procedures around release of Notice of Penalty "cover pages"? Does SERC agree or disagree that release of the entity names, standards, and fine amounts increases risk to utilities?

RESPONSE: SERC and the other Regions worked closely with NERC and FERC on the White Paper. While the final proposal does not completely align with SERC's desired outcome, SERC believes the final White Paper balances potential risk with the desired transparency. SERC does not plan on submitting comments but encourages entities to do so. Comments are due by October 28, 2019.

11. Is a VPN considered an intermediate device? A VPN connection is required to connect to the ESP.
Clarification: Is a VPN considered an intermediate device? A VPN connection is required to connect to the ESP.

RESPONSE: An Intermediate System is a Cyber Asset or collection of Cyber Assets to perform Interactive Remote Access to authorized users that is not located inside the Electronic Security Perimeter. A virtual private network (VPN) extends a private network across a public network by using encryption to protect the data. CIP Reliability Standard CIP-005-5, Requirement R2, Part 2.1 requires the use of an Intermediate System for all Interactive Remote Access sessions. CIP Reliability Standard CIP-005-5, Requirement R2, Part 2.2 requires all Interactive Remote Access sessions to "utilize encryption that terminates at an Intermediate System." A VPN is often used to provide the encryption that terminates at an Intermediate System. However a VPN is in not an Intermediate System in itself, rather a possible component to an Intermediate System.

12. Under CIP 10 1.1.4 Custom Software, it is our understanding that SERC considers Custom scripting as Installed software. Under the SERC FAQs, it was stated that monitoring the directory was placed into was not acceptable. If this software was intentionally installed, why is this unacceptable?

Under review. Response to be posted upon receipt.

13. We had a recommendation that internet access be removed from a server that updates anti-virus updates, what would be the preferred method to get updates to the ESP?
Clarification: We had an audit recommendation that internet access be removed from a server that updates anti-virus signatures, what would be the preferred method to get antivirus updates to the ESP?
RESPONSE: As a compliance enforcement authority, it is not appropriate for SERC to give a preferred method. We are aware of several sources that could provide guidance to registered entities on good related security practices including, but not limited to the ICS CERT Recommended Practice on Updating Antivirus in an Industrial Control System as well as similar publications from NIST such as 800-83... In addition a request could be made to SERC Assistance for their recommendations.

14. What evidence is a Responsible Entity expected to provide for CIP-003-7 R2 Attachment 1 Section 5 compliance engagement that would enable an auditor to identify instances wherein an entity permitted a TCA/RM to be connected to a BCA/PCA for longer than 30 days?

Under review. Response to be posted upon receipt.

15. Renny: In your presentation, you noted that a low TCA connected to a low BCS for more than 30 days is a violation. Can you please provide the requirement under CIP-003 R2 that states it is prohibited for a TCA to be connected for more than 30 days? What if an Entity intends to have devices connected to low BCS for more than 30 days, more than 3 months, etc.?

- Guidance from NERC and FERC has been that a TCA connected for more than 30 days would become a component of the low BCS it is connected to, and must be afforded the same protective measures of the low BCS. They, along with the NERC CIP SDT, recognize that there is no current classification for a low TCA connected to a low BCS for more than 30 days – it's undefined. The comment from NERC today implying that the TCA becomes a PCA was incorrect in that a PCA implies there is an ESP, by definition, which is not required for lows. There is also no requirements under CIP-003 R2 that are applicable to PCAs, so even if a TCA became a PCA, there are no requirements for which an Entity could be non-compliant with for that device. Additionally, there is no requirement or prohibition stating that a low TCA cannot be connected to a low BCS for more than 30 days, so how is SERC justifying assessing a PV for such a case?

You also mentioned that a low TCA connected to a low BCS for more than 30 days would be a violation because it would fall out of patch cycles. Can you please provide the requirement under CIP-003 R2 that requires low TCAs to be patched at least once every 30 days? Or at all?

Under review. Response to be posted upon receipt.