## DRAFT CIP V5 Implementation Issues

<table>
<thead>
<tr>
<th>Topic</th>
<th>SAR Comments: The SDT should also consider …</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CIP Exceptional Circumstances</td>
<td>A CIP Exceptional Circumstance is defined as:</td>
</tr>
<tr>
<td></td>
<td>“A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.”</td>
</tr>
<tr>
<td></td>
<td>Industry appreciates the understanding and recognition for the need to enable provisions for CIP Exceptional Circumstances. However, during implementation of CIP V5, it has become apparent that the CIP Exceptional Circumstances provision may need to be added to several requirements. Below are a few situation-based examples:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Risk of injury or death:</strong> CIP-004-6 R2 and R4 allow for CIP Exceptional Circumstances to waive the need for Training and the Authorization based on need to be waived during such circumstances. We believe that CIP-004-6 R3 also should allow for CIP Exceptional Circumstances because the requirement to obtain a Personal Risk Assessment takes additional time that would hinder the ability of first responders to enter a Physical Security Perimeter in the event of the need for life saving measures. This would be consistent with CIP-004-3 “except in specified circumstances such as an emergency.”</td>
</tr>
<tr>
<td></td>
<td>• <strong>Impediment of large scale workforce availability:</strong> CIP-007-6 R2 Security Patch Management requirements may be difficult to meet in the event that a major storm impacts a responsible entity, which requires all employees to report for storm duty for restoration efforts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Natural disaster:</strong> CIP-006-6 R1 Part 1.4 monitoring may not be possible if the physical access point to a PSP is under water or destroyed by a storm. Similarly, Part 1.3 causes compliance issues if for example, a fire renders a PACS controller panel inoperable and the PSP access points have failed secure. Emergency response may have to use a physical key, mechanical lock, or an axe to gain access. Without the IAC language or CIP Exceptional Circumstance provision, PSP access point monitoring is a zero defect issue.</td>
</tr>
</tbody>
</table>

We recommend that the SDT review all of the requirements of CIP V5 to determine whether: a CIP Exceptional Circumstances provision should be added, the definition of CIP Exceptional Circumstances should be edited, and/or additional explanatory language should be added to the Guidelines and Technical Basis for each standard regarding CIP Exceptional Circumstances.
2. **BES Cyber Asset definition – “redundancy”**

The application of the redundancy clause in the BES Cyber Asset (BCA) definition is unclear because the use of different and separate technologies and methods reduce reliability risk by providing alternative data sources. For example, VoIP systems, data center phone systems, radios, and other backup communication systems are alternatives, yet could be considered redundant by auditors and therefore it is unclear whether there are limits to the application of the BCA adverse impact to these systems. Without such limitations, the BCA definition may encourage registered entities to reduce their use of backup/alternative systems to reduce their compliance burdens and risk. While redundant assets may typically have identical security risks and vulnerabilities, requiring both/all to be similarly protected, alternative systems or assets are often substantially different and have drastically dissimilar risks and vulnerabilities, which reduces overall risk to the BES.

3. **VoIP as a BES Cyber Asset**

CIP-002-5.1 4.2.3.2 exempts “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters” from CIP-002-5.1; however, the Guidelines and Technical Basis for CIP-002-5.1 calls out operational directives (TOP, RC, BA) as an aspect of Inter-Entity Coordination and Communication function. As a result, some auditors are viewing VoIP as in scope for CIP-002-5.1 despite the exemption and fact that different and separate communication technologies are used for this function. If the exemption does not apply, then the BES Cyber Asset definition should also apply; however, EEI members are hearing that auditors do not agree and believe that VoIP used for operational directives are BES Cyber Assets even if the 15 minute impact does not apply due to the redundancy issue mentioned above.

We recommend that the SDT consider these issues and determine how best to address VoIP in the standard that is aligned with the risk to the bulk electric system.

4. **LERC definition application to assets located external to the low impact asset**

The last three asset classes in CIP-002-5.1 R1 are typically implemented across multiple instances of the first three classes (i.e., systems and facilities critical to system restoration, special protection systems, and distribution provider protection systems are typically implemented at control centers, substations, and generating resources).

The Low Impact External Routable Connectivity (LERC) definition appears to be based on single asset locations (“direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.”) The phrase “outside the asset” can cause confusion in determining whether LERC exists for these classes of assets that are implemented across multiple sites.

For example, when evaluating a cranking path as an asset to determine if it has LERC, what does “outside the asset” mean? This could also allow for routable protocol based communication within the multiple substation cranking path to not be considered LERC and left unprotected if the entire cranking path is considered a single “asset containing low impact BES Cyber Systems.” It appears these last 3 asset classes are actually criteria that should affect the categorization of the single site asset class where they are implemented.
5. Custom software (scripts)  
CIP-010-2 R1, Part 1.1, subpart 1.1.3 requires a baseline configuration for “any custom software installed”  
The Guidelines and Technical Basis for this requirement states that “custom software installed may include scripts developed for local entity functions.” It is unclear whether all scripts must be considered custom software or whether only scripts that can have an impact on the bulk electric system within 15 minutes must be considered custom software under this requirement. A risk-based clarification should be added to this requirement to set boundaries as to what is considered custom software. For example, a script that alters the behavior or function of a BES Cyber Asset or System should be included; however, a script that simply gathers log data, and whose only impact to the BES Cyber Asset is the allocation of incidental CPU cycles, need not be included.

6. Applicability of the requirement part to Cyber Asset vs. Cyber System  
Some requirements such as in the CIP-007-6 standard apply to Cyber Assets within a BES Cyber System (e.g., the R2 security patch management requirements), others apply at either the BES Cyber System level or Cyber Asset level (e.g., the R4 Part 4.1 logging requirements), and others don’t specify if they apply at the system or asset level (e.g., R3 Part 3.1 method to deter, detect, or prevent malicious code). Although the applicable systems for each of these requirements is generally the same (i.e., high and medium impact BES Cyber Systems and their associated EACMS, PACS, and PCA), the difference in the requirements language applicability to Cyber Assets, BES Cyber System, or both makes what is necessary to comply with the requirements unclear.  

For example, the requirements section for CIP-007-6 R3 Part 3.1 does not specify whether this requirement applies at the BES Cyber System level or Cyber Asset level, therefore it is unclear whether a responsible entity can protect a medium impact BES Cyber System through deploying an anti-virus solution at the BES Cyber System level or whether the entity must deploy the solution at each Cyber Asset to comply with the requirement part. Consistency among the requirements language would be helpful in clearing up this confusion.

7. Control Center definition  
The NERC document titled “CIP V5 Issues for Standard Drafting Team Consideration” already raises issues with the Control Center definition related to Transmission Owner Control Centers; however, it does not address issues related to Generator Operators.  

By definition, a Control Center is “one or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers … 4) a Generator Operator for generation Facilities at two or more locations.”  

Dispersed or distributed generation facilities (e.g., wind, solar, hydro) may not have the traditional control building with a horseshoe operator control desk (“facility hosting operating personnel that monitor and control”). Does the facility have to perform all “real-time … reliability tasks” or as few as one? Does a control room at a single wind farm, which controls a hundred turbines spread over many miles, meet the control center definition or does it become a control center only if it controls multiple wind farms? Also, if personnel maintains the Cyber Assets (e.g., patching or troubleshooting) is this considered “monitor and control” even though they are not personnel performing real-time reliability tasks. Does operating personnel mean those charged with the
responsibility to monitor and control the BES or simply personnel who may be located at the generation Facility to maintain the equipment? Also, do each of the “generation Facilities at two or more locations” need to meet the Bulk Electric System definition to be within scope of the Control Center definition? CIP-002-5.1 Requirement R1, iii uses Generation resources, which could be interpreted to include all generation sources, even those that do not meet the Bulk Electric System definition.

As dispersed or distributed generation increases, clarity in language of the standard will become more important.

<table>
<thead>
<tr>
<th>8. Security patches for operating Cyber Assets brought into scope under CIP V5</th>
</tr>
</thead>
</table>
| **CIP-007-6 R2**, Part 2.2 is clear concerning the ongoing evaluation of security patches as of July 1, 2016, but is unclear on what is required for the initial execution of the process (“evaluate security patches for applicability that have been released since the last evaluation”) when there is no “last evaluation.”

The standard does not require all Systems to be updated by July 1, 2016, but does require a baseline configuration, which includes a listing of all applied patches. The Guidelines and Technical Basis for CIP-010-2 states that “security patches applied would include all patches that have been applied on the cyber asset… CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.” This documentation requirement is particularly burdensome for an asset that has been in service for six years or longer as it requires entities to contact and work closely with their vendors to identify and get historical security patches. Also, documenting all historical patches, especially those that happened years ago will have little, if any impact on reliability.

|-----------------------------|
| In the Guidelines and Technical Basis for CIP-005-5, under Requirement R2 it states: “see Secure Remote Access Reference Document (see remote access alert).” Also, the Rationale for R2 states “Additional information is provided in Guidance for Secure Interactive Remote Access published by NERC in July 2011.” We believe these references are to the same document, which is properly titled under the Rationale and note that the 2011 NERC document was written in the context of V3 and not V5. Please evaluate the relevance of this guidance document to the most recent version (currently CIP-005-5). Also please clarify that IRA is intended to address access remotely from outside the organization (i.e., not to include accesses internally between protected networks).

<table>
<thead>
<tr>
<th>10. Mistakes in Guidelines and Technical Basis</th>
</tr>
</thead>
</table>
| In implementing CIP V5, we’ve noticed a number of mistakes, which should be addressed, including:

- The rationale statements from the -5 standards were lost in several of the -6 versions of the standards. For example, the second sentence of the CIP-007-5 R2 rationale “The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.” was not carried forward to the -6 Guidelines and Technical Basis, even though there were no changes to the requirement between versions. We recommend reviewing the Rationales in the -6 standards and adding any that were deleted to the Guidelines and Technical Basis of the standard.

- For CIP-007-6 Part 2.2 the Guidelines and Technical Basis states: “Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the
system configuration should not require a TFE.” However there are no CIP-007-6 R2 Parts have TFE provisions.

- For CIP-004-6 R4, under the Guidelines and Technical Basis, the Rationale for this requirement states: “to ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. ‘Authorization’ should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6” CIP V3 required designating approvers; however this requirement was not included in CIP-003-6 and therefore the emphasized text should be removed.

- For CIP-004-6 R4, the Rationale also references “quarterly reviews in Part 4.5”; however there is no Part 4.5 in CIP-004-6 R4.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Issues to Monitor (not for the SAR comments)</th>
</tr>
</thead>
</table>
| 1. CIP-002-5.1, Criteria 2.6 Att 1: IROLs (from April 2015 CAMs) | This was one of the April 2015 Compliance Assurance Memorandums, which has not yet been resolved regarding Impact Rating Criteria 2.6.  

Criteria 2.6 for “generation at a single plant” is the area of question. For Attachment 1 criteria 2.6, the RC/TPs identify the Facility. Identification of the right BES Cyber Systems/Cyber Assets for CIP-002-5 R1.2 by the GO/GOP may not occur if the RC/TPs only identify the Facility. The RC/TP’s know which Facilities and system(s) are critical to the derivation of the IROLS. Therefore, their notification to the GO/GOPs should include not only the Facility, but the system(s) as well. For example, two ISOs have identified knowledge of the status of AVR as important to having an impact on the limit.

Thus far, the issue has been identified in the New York ISO and New England ISO regions (2.6 criteria for generation units—approximately 25 units impacted).

Other ISOs/RTOs may identify other system(s) that are critical to derivation of IROLS. RC/TP should define the system(s) that is/are critical to derivation of IROLS. The GO/GOP should identify BES cyber assets and BES cyber system(s).

Additional data/information is needed from the planning engineers that understand the issue:
- (IROLs derivation) FAC-014-2 R5.1.1 and .3 (not all IROLs are alike); and,
- VAR-002-4 R3 and R4 (which has 30-minute parameters).

Note: Two ISOs have identified the AVR system is critical to the derivation of IROLS” since its status has an impact on the limit. When AVR’s are removed from service, including the unit being taken out of service, the
IROL Limit is reduced. Also, derivation of IROLs and their associated contingencies often considers the effect of generation inertia and the AVR response.

Recommendation to NERC was to issue a FAQ to allow RC/TP to identify system(s) at the Facility that are critical to the derivation of the IROL.

2. Interactive Remote Access – “management consoles”

The draft Lesson Learned dated April 29, 2015 contained the following bullet:

- Responsible Entities should determine whether management consoles are used to provide Interactive Remote Access. If a management console allows a remote user to access, configure or update BES Cyber Systems within an ESP, then the management console must be considered an Intermediate System or part of an Interactive Remote Access process to which the CIP Version 5 requirements for Interactive Remote Access would apply.

EEI commented that this bullet expands the scope of the Interactive Remote Access requirements. The Interactive Remote Access requirements were intended to address security risk associated with remote computers using Virtual Private Network (VPN) technology. In voting for the CIP CIP-005-5, Registered Entities were aware of the VPN risk, but had not considered management consoles as Intermediate Systems which is introduced by this Lesson Learned. Section 11 guidance should not modify the requirements of CIP-005-5.

The appropriate mechanism for expanding the scope of a standard is through the standards development process. If security risks have been identified through transition program activities, then these issues should be articulated to the standards drafting team and considered in a standards revision process.

Due to this concern, EEI recommended deleting this bullet or revising it as follows:

- Responsible Entities should consider their specific facts and circumstances and evaluate and manage potential security risks associated with management consoles. In some scenarios, an entity might determine that it is appropriate for them to consider a management console as an Intermediate System.

The IRA Lesson Learned has not been finalized by NERC so this remains an issue to monitor.

3. Tie line meters as BCAs

Whether tie line meters are BES Cyber Assets will depend upon how the data reported by the meter is used. For example, if it’s used for real-time situational awareness, then the Cyber Assets associated with the metering will likely be a BCA. However, if the data is used for purely financial reasons, it will not be a BCA. There is concern that NERC and/or the Regions may be supporting an interpretation that tie line meters should be categorized by the impact rating of the substation they are physically located at, this is similar to the far-end relay issue. However, the difference is that far-end relays are associated with the reliable operation of the substation they are located at, whereas with tie line meters, they may not be associated with the reliable operation of the substation they are located at. To be a BCA, the tie line meter must meet the BCA definition. It is understood by industry that some tie line meters may be BCAs while others may not. This issue originated with an FAQ related to tie line meters with dial-up modems. EEI suggested a sentence change from the proposed answer to read: “if the data
reported by a metering system is used for real-time situational awareness, then the Cyber Assets associated with the metering will likely be medium or low impact…” However this FAQ was never finalized.

For some locations, tie line meters may be reporting data used in ACE calculations. Would this automatically mean that because the data is used for ACE (Balancing Load and Generation) that the device would be considered a medium impact BCA even if the real-time tie flow is coming from an asset that has been identified as one containing low impact BCS.