

Consideration of Comments on Initial Ballot of Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets for South Carolina Electric and Gas

Summary Consideration: The drafting team did not make any changes to the interpretation based on the comments submitted with the initial ballot of the interpretation of CIP-006-1.

Organization:	Alberta Electric System Operator
Member:	Anita Lee
Comment:	<p>This interpretation is rendered awkward due to the highly prescriptive nature of the CIP-006 standard. The standard overlooks the overall objective, that being adequate physical security for critical cyber assets, and attempts to addresses details that mislead the safeguard selection process.</p> <p>Specifically, the matter of routable protocols being used by the critical cyber asset is not particularly salient to the determination of the adequacy of physical security measures. Furthermore, prescribing a six-wall border compounds the difficulty of arriving at an appropriate conclusion, by forcing even more implementation level detail into consideration. Consequently, on one hand, the interpretation seems acceptable, in the sense that a six-wall border is not absolutely necessary for dialup RTUs that do not use routable protocols. However, this point is specious, since the same could be said for any critical cyber asset.</p> <p>If appropriate alternative measures are in place to provide physical security, then the use of routable protocols and the presence of six-wall borders are unnecessary details and should therefore not be considered at the level of a generic, mandatory standard. However, on the other hand, the interpretation is not acceptable, in the sense that it fails to indicate that appropriate physical security measures must be implemented, regardless of the use or lack of routable protocols. This ambivalence is caused directly by the standard approaching a level of detail that can only be properly considered in a specific circumstance, not in the general case.</p>
Response:	While the comments directed at the standard are appreciated, the interpretation focuses on the standard as approved. The interpretation is consistent with the set of cyber security standards in that it provides a balanced solution between not having any protection (as would be the case for a non-dial-up, non-routable connection), and “full” protection for a permanently-connected routable protocol connection.
Organization:	Consumers Energy Co.
Member:	David A. Lapinski
Member:	David Frank Ronk
Comment:	We are voting in favor of this interpretation, but we recommend that the phrase, “and they must reside within an Electronic Security Perimeter” should be omitted. This interpretation is nominally related only to CIP-006-1. This phrase seems to bring CIP-005 into the scope of the interpretation. It appears that the phrase was included solely for illustrative reasons in the original interpretation request. Repeating it in the formal interpretation, however, raises a number of concerns regarding CIP-005 interpretation. We believe these are unintended and may be inconsistent with CIP-005 and its associated explanatory documentation (such as the FAQ’s).
Response:	The phrase was included for illustrative purposes to remind the reader that Electronic Security is still required. For compliance purposes, only the requirements of CIP-005 may be used to assess compliance. CIP-006, its interpretation, or any element of the

Consideration of Comments on Initial Ballot of Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets for South Carolina Electric & Gas

	FAQ cannot be used to establish new requirements, or to assess compliance.
Organization:	Lincoln Electric System
Member:	Bruce Merrill
Member:	Dennis Florum
Comment:	LES agrees with the interpretation as written, however it is not needed. As the Interpretation team has correctly pointed out, South Carolina Electric & Gas's query is already addressed in Additional Compliance Information 1.4.4 of the standard. Per the Reliability Standards Development Procedure, a interpretation will stand with the approved standard until the standard is revised through the normal process, at which time the standard will be modified to incorporate the clarifications. It seems unnecessary for this Interpretation to stand with the currently approved standard and additionally no modifications to the approved standard appear to be needed as a result of this Interpretation.
Response:	The formal Request for Interpretation process obliges NERC to prepare, post for review and ballot a response to the request. The requestor sought a formal interpretation therefore the process was initiated and followed. The resultant interpretation response confirmed the intent of the drafting team, and may be used during revisions of the CIP-006 standard as justification for clearing up any language or confusion in the standard.
Organization:	Electric Reliability Council of Texas, Inc.
Member:	Kent Saathoff
Comment:	The interpretation should not be approved because it could create a situation where a Critical Cyber Asset could be left unprotected outside of a Physical Security Perimeter or Electronic Security Perimeter.
Response:	The interpretation does not eliminate the requirement for an Electronic Security Perimeter (in specifically reminds the reader that the assets must reside within an Electronic Security Perimeter). The interpretation is consistent with the set of cyber security standards in that it provides a compromise solution between not having any protection (as would be the case for a non-dial-up, non-routable connection), and "full" protection for a permanently-connected routable protocol connection.
Organization:	Southwest Power Pool
Member:	Charles H. Yeung
Comment:	<p>There is an alternative already identified in CIP-006 that SCE&G can apply to its dial-up RTUs in a facility that is difficult to secure.</p> <p>From Page 18 of the CIP standards FAQ: Standard CIP-006-1 — Cyber Security — Physical Security 1. Question: What is a "six-wall" border? Answer: This refers to a physical, completely enclosed border, such as a room, cage, safe, or metal cabinet. Raised floors and drop ceilings may not constitute part of a border because they could create potentially uncontrolled access points. Fences do not constitute a completely enclosed border. The intent is to clearly define a security boundary that applies the same level of security over its entire area.</p> <p>However, SPP is aware that this interpretation may be based on wording from Sec D. Compliance: 1.4. Additional Compliance Information 1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.</p> <p>SPP is concerned that D.1.4.4 and the interpretation diminishes the purpose of CIP-</p>

Consideration of Comments on Initial Ballot of Interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets for South Carolina Electric & Gas

	<p>006, whereas the FAQ quoted provides appropriate cyber security protection and a reasonable solution for securing a dial-up RTU that is recognized by the registered entity to be a critical cyber asset. Compliance information should not be applied to contradict the purpose of the standard itself. Although the interpretation is limited to the existing standards language, and the NERC standards process should be used to submit a standards change, SPP does not support this interpretation.</p>
<p>Response:</p>	<p>The requestor sought a formal response to its request for interpretation. The interpretation is based in the language of the Compliance section noted. The FAQ is an informational-only document, and does not contain any requirements. Since the interpretation is based on language already included in the standard, there are no new requirements or changes to existing requirements.</p>