NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: A valid interpretation request is one that requests additional clarity about one or more requirements in approved NERC reliability standards, but does not request approval as to how to comply with one or more requirements.

When completed, email this form to:
laura.hussey@nerc.net
For questions about this form or for assistance in completing the form, call Laura Hussey at 404-446-2579.

Request for an Interpretation of a Reliability Standard	
Date submitted: December 8, 2011	
Contact information for person requesting the interpretation:	
Name: Thad Ness	
Organization: American Electric Power Service Corp	
Telephone: 614-716-2053	E-mail: tkness@aep.com
Identify the standard that needs clarification:	
Standard Number (include version number, e.g. PRC-001-1): CIP-005-3	
Standard Title: Cyber Security — Electronic Security Perimeter(s)	
Identify specifically what requirement needs clarification:	
Requirement Number and Text of Requirement: R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	
Identify the nature of clarification that is requested: (Check as many as applicable)	
☒ Clarify the required performance ☒ Clarify the conditions under which the performance is required ☐ Clarify which functional entity is responsible for performing an action in a requirement ☒ Clarify the reliability outcome the requirement is intended to produce	
Please explain the clarification needed: For the purposes of access point identification, do “externally connected communications endpoints” include those communications links that do not use either	

(1) a routable protocol (such as IP), or (2) a dial-up modem?

Specifically, does a Communications Front End Processor (or one of its peripherals) that resides within an ESP and is used to communicate directly via non-dial-up serial link with substation RTUs via non-routable protocol need to be identified as an ESP access point?

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others, if known, caused by the lack of clarity or an incorrect interpretation of this standard.

There are certain types of external connections for which compliance with CIP-005-3 poses a significant problem if the systems supporting these connections were to be identified as ESP access points.

Identification of the serial links on Communications Front End Processors (which use neither a routable protocol, nor a dial-up modem) as ESP access points result in compliance problems for CIP-005-3, requirements R2, R3 and R4.

The following requirements in CIP-005-3 apply to ESP access points, but are not technically feasible for the Communications Front End Processors (or associated peripherals) and no TFE is permitted:

- R2.1 – not technically feasible, no TFE permitted
- R2.2 – not technically feasible, no TFE permitted
- R2.3 – not technically feasible, no TFE permitted
- R2.5 – not technically feasible, no TFE permitted
- R4.2 – not technically feasible, no TFE permitted
- R4.3 – not technically feasible, no TFE permitted

Responsible Entities understand that it is not possible to simply list a requirement as "Not Applicable" or "N/A" – the Responsible Entity must be either strictly compliant (and have evidence demonstrating as such) or have a TFE on-file. As illustrated above, it is not possible to be strictly compliant with several access point requirements if these devices were to be identified as ESP access points, and yet it is not possible to take a TFE on those requirements.

The lack of clarity around CIP-005-3, R1.1 (or worse, the incorrect interpretation) results in a lack of rigor for CIP-005-3, R2. Clarifying the scenarios where CIP-005-3, R1.1 applies would result in more uniform, rigorous and predictable compliance with CIP-005-3, R2.