

**Project 2009-13: Interpretation of CIP-006-1 for PacifiCorp  
Consideration of Comments on Initial Ballot (conducted August 27–September 8, 2009)**

**Summary Consideration:** Of the negative ballots with comments, the majority noted disagreement with the drafting team’s interpretation that wiring is a component of a communication network and needs protection. The drafting team explained that the definition of Cyber Assets in the NERC Glossary of Terms Used in Reliability Standards (Glossary) includes communication networks, and the physical media (wiring) is a component of the communication network.

A minority of comments expressed disagreement with the interpretation that alternate measures include logical methods. The drafting team believes logical methods to be within the spectrum of potential alternate measures for CIP-006-1.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.<sup>1</sup>

Voter	Entity	Segment	Vote	Comment
Gordon Rawlings	BC Transmission Corporation	1	Negative	BCTC’s interpretation, through reading the requirements, is that cyber assets are those that are IP addressable (routable) or accessible via hard lines (i.e. telephone or modem); wiring is neither.
Faramarz Amjadi	BC Transmission Corporation	2	Negative	BCTC’s interpretation, through reading the requirements, is that cyber assets are those that are IP addressable (routable) or accessible via hard lines (i.e. telephone or modem); wiring is neither.
<p><b>Response1:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an Electronic Security Perimeter (ESP), but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p>				
Robert Martinko	FirstEnergy Energy Delivery	1	Negative	FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised."

<sup>1</sup> The appeals process is in the Reliability Standards Development Procedure: [http://www.nerc.com/files/RSDP\\_V6\\_1\\_12Mar07.pdf](http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf).

Voter	Entity	Segment	Vote	Comment
Joanne Kathleen Borrell	FirstEnergy Solutions	3	Negative	FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised."
Kenneth Dresner	FirstEnergy Solutions	5	Negative	FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised."
Mark S Travaglianti	FirstEnergy Solutions	6	Negative	FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised."
Douglas Hohlbaugh	Ohio Edison Company	4	Negative	FirstEnergy is voting NEGATIVE to the interpretation response as we do not believe it fully addresses the issues raised by PacifiCorp. The interpretation response provided only addresses the Electronic Security Perimeter (ESP) wiring external to a Physical Security Perimeter (PSP) and not alternative measures to control physical access to Critical Cyber Assets that may not reside within a "six-wall" physical border. The question posed by PacifiCorp relates to Critical Cyber Assets, not simply the ESP wiring. As such, the interpretation provided does not meet the NERC Reliability Standard Development Procedure which states " ...the team will draft a written interpretation to the standard addressing the issues raised."

**Response2:** The drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection. The requester describes their topology as such therefore the drafting team addressed the issue as stated.

Voter	Entity	Segment	Vote	Comment
<p>CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border. For ESP wiring that is external to the PSP: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or monitoring to detect unauthorized access or physical tampering.</p>				
James R. Nickel	Michigan Public Power Agency	5	Negative	MPPA does not believe the intent of R1.1 was to classify wiring as a Cyber Asset subject to the CIP requirements. The term "Cyber Asset" refers to those components to which the wires are connected, such as patch panels, routers, switches etc. MPPA is not arguing that the wiring is irrelevant or unimportant, but contends that it should be handled separately from the existing CIP Standards.
<p><b>Response3:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p>				
Gregory D Maxfield	PacifiCorp	6	Negative	<p>Regarding PacifiCorp’s requested interpretation of CIP006.R1.1: Our primary concern was commentary from some industry participants who took the view that the phrase “..to control physical access” as used in CIP006.R1.1 represented a requirement for a control that would literally prevent physical access. This viewpoint was not a consensus opinion, but if left unchecked might percolate into the auditor ranks and represent a compliance risk to entities needing to use logical controls as an “alternative measure”. Hence, we took the proactive action of requesting an interpretation from the drafting team. Entities should support this interpretation as it is simply a clarification that entities have the option to use logical controls as alternative measures for CIP006.R1.1.</p> <p>Regarding the posted interpretation of CIP005.4.2.2 and CIP005R1.3: Our primary concern was a distinct lack of clarity around the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links”. Unfortunately, the proposed interpretation provides no meaningful clarity. We recommend that entities not support this provided interpretation.</p>
<p><b>Response4:</b> Thank you for your comment. The drafting team agrees with your position that controlling physical access may encompass both logical and physical measures.</p> <p>In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>				
Trent Carlson	RRI Energy	6	Negative	RRI Energy votes negative in support of PacifiCorp's position. PacifiCorp’s primary concern was a distinct lack of clarity around the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links”. Unfortunately, the proposed interpretation provides no meaningful clarity.

Voter	Entity	Segment	Vote	Comment
<p><b>Response5:</b> In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>				
Jonathan Appelbaum	Long Island Power Authority	1	Negative	The interpretaion team needs to explain what the purpose of a six wall border is and measures for effectiveness. Then the effectiveness of an alternative implemetaion to a six wall border can be measured. For example, is the purpose of a the border to encourage persons to enter thru monitored access points, or is it hardened protection? Once measures are provided then logical controls and alternative methods can be evaluated for effectiveness by the entities.
<p><b>Response6:</b> The drafting team provided an interpretation for the issue requested and does not have the latitude to go beyond what is requested.</p>				
Louise McCarren	Western Electricity Coordinating Council	10	Negative	The interpretation introduces the option of logical controls where a six-wall border cannot be established. This removes some uncertainty surrounding the language of R1.1. However, a negative vote is being cast for the following reason. Clarification should be provided as to whether the term "wiring" is intended to be exclusive literally to physical wires, or more expansively to communication paths, including intermediate devices such as repeaters, bridges, frame relay devices, MPLS nodes, etc. Clarification should be provided with respect to the particular elements of security which need to be provided (i.e. confidentiality, integrity, availability). If additional clarity is provided we would support this interpretation.
<p><b>Response7:</b> The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.</p>				
Hubert C. Young	South Carolina Electric & Gas Co.	3	Negative	The question being asked is broader than just the location of the wiring that makes up part of the ESP. The interpretation should address the questions of 1) what constitutes appropriate "alternative measures" if a physical six-wall boundary cannot be established? (motion detectors, video cameras, others) and 2) what is meant by "control"? Also, how can a logical measure be equivalent or better than a physical measure? After all, no matter how encrypted the connection or how well the circuit is monitored via a security system, couldn't someone just cut the cable?
<p><b>Response8:</b> CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p>				

Voter	Entity	Segment	Vote	Comment
Richard Jones	South Carolina Electric & Gas Co.	5	Negative	The question being asked is broader than just the location of the wiring that makes up part of the ESP. The interpretation should address the questions of: 1) What constitutes appropriate "alternative measures" if a physical six-wall boundary cannot be established? (motion detectors, video cameras, others), and 2) What is meant by "control"? In addition, how can a logical measure be equivalent to or better than a physical measure? No matter how encrypted the connection or how well the circuit is monitored via a security system it doesn't stop someone from physically cutting a cable.
<p><b>Response9:</b> CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p>				
Michael Gammon	Kansas City Power & Light Co.	1	Negative	The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.
Charles Locke	Kansas City Power & Light Co.	3	Negative	The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.
Thomas Saitta	Kansas City Power & Light Co.	6	Negative	The response to question 3 is confusing and introduces ambiguity into the standards. A thorough analysis of the implications of defining endpoints as either physical or logical and the resulting impact on the rest of the standards has not been completed.
<p><b>Response10:</b> In regard your comment on endpoints, the drafting team refers you to the response to comments for Project 2009-12: Interpretation of CIP-005-1 – Cyber Security – Electronic Security Perimeters for PacifiCorp.</p>				
Jason L. Murray	Alberta Electric System Operator	2	Negative	This interpretation would change the standard by allowing the use of safeguards that cannot control physical access, as required by the standard. An interpretation cannot be used to change a standard, and this interpretation would have that effect.
<p><b>Response11:</b> The RFI response drafting team interprets "alternative measures" for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection.</p> <p>CIP-006 R1.1 states: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.</p>				

Voter	Entity	Segment	Vote	Comment
Kim Warren	Independent Electricity System Operator	2	Negative	While CIP-006-1, Requirement R1.1 clearly requires physical measures, it does not reference logical measures. Thus, our view is that this interpretation effectively alters the requirement, rather than interprets it, with the words “physical or logical” and “Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.” Although we believe the standard should be revised to allow alternative protective measures, doing so within the context of an interpretation is inconsistent with the Reliability Standards Development Procedure. We are therefore of the view that the interpretation needs more work.

**Response12:** The RFI response drafting team interprets “alternative measures” for ESP wiring that is external to the PSP to include use of a combined/complementary physical or logical approach to achieve the same or better protection.

CIP-006 R1.1 states: “Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.” The alternative measures for ESP wiring that is external to the PSP may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed (“six-wall”) border: alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space; alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Alan Gale	City of Tallahassee	5	Negative	While we agree that "alternate logical control measures" should be allowed, we feel the interpretation is still forcing the "wiring" of a "communication network" into the list of what is a Cyber Asset". This we vehemently disagree with.
-----------	---------------------	---	----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Response13:** The definition of Cyber Asset in the NERC Glossary includes communication networks. The interpretation response team has reviewed its response and considers the physical media (wiring) a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset; therefore, the network wiring needs to be protected.