NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2009-12: Interpretation of CIP-005-1 — Cyber Security — Electronic Security Perimeters for PacifiCorp
Consideration of Comments on Initial Ballot (August 27–September 8, 2009)

Summary Consideration:

There were mainly two themes that the commenters raised. First, there were comments that pertain to lack of clarity around the issue of access point identification. Second, some commenters questioned the interpretation on tunnels that have termination point beyond an Electronic Security Perimeter (ESP) access point.

The drafting team response to the first theme clarifies that an encrypted tunnel that originates from outside of the ESP and terminates within or at the ESP is an access point. The drafting team offers that encrypted data cannot be adequately inspected at an upstream access point, such as a firewall, in order to provide the required level of protection. Therefore, the termination point must be considered an access point to the ESP and must be protected per CIP-005.

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.[1]

Voter	Entity	Segment	Vote	Comment
James L. Jones	Southwest Transmission Cooperative, Inc.	1	Negative	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.The interpretation is still hazy in my mind.
Response1: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.				
Donald S. Watkins	Bonneville Power Administration	1	Negative	BPA believes the interpretation wording of Question 4 that "the termination points of an encrypted tunnel must be treated as an "access point"" is too restrictive and will conflict with other interpretations. Specifically the PACW request for interpretation of CIP-006-

[1] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Voter	Entity	Segment	Vote	Comment
Rebecca Berdahl	Bonneville Power Administration	3	Negative	01, the use of data encryption as an alternate measure for physical protection, is meant to allow creating one ESP that spans multiple PSPs. With this CIP-005-01 interpretation, it could be interpreted that all encrypted tunnels are an access point to an ESP. BPA provides the following non-directive comment in regard to the scenario given in Question 4: if the encrypted tunnel is connecting two discrete ESPs, then the ends of link (logical or physical) must be considered access points in accordance with CIP-005-1 R1.1. However, the architecture described in the question could also be interpreted as a single ESP consisting of the individual ESPs at each control center and the link connecting them. In this case, the encryption serves to provide an alternative means of physical protection, as described in the response to Pacificorp's Request for Interpretation for CIP-006-1 . The encrypted link is entirely internal to the PSP and the ESP; and CIP-005 is not relevant. No endpoints exist.
Francis J. Halpin	Bonneville Power Administration	5	Negative	
Brenda S. Anderson	Bonneville Power Administration	6	Negative	
Response2: Thank you for your comment. The encrypted tunnel envisioned as an alternative protective measure for CIP-006-1 extends a single ESP across two geographically separate Physical Security Perimeters (PSPs). In that instance, as the encrypted tunnel is a closed link between the two PSPs and all traffic across that tunnel is contained within a single ESP, the tunnel endpoints would not be considered ESP access points. However, the question asked in this interpretation request is in regard to an encrypted tunnel connecting two distinct ESPs without respect to any PSP containment. In this instance, the endpoints of the encrypted tunnel are the access points to the respective ESPs and must be protected per the requirements of CIP-005-1.				
Russell A Noble	Cowlitz County PUD	3	Negative	Cowlitz PUD votes negative for the following reasons: Answer to Question 2 fails to clarify where a communication link begins and terminates. Cowlitz understands a communication link can be physical and/or logical. However, the interpretation needs to go further than stating the termination points depend on design and architecture. At the very least, three common design scenarios could be explored and termination points defined in each example. Without some guidance, entities are left to guess and hope the auditor will agree. Question 4 is confusing, but Cowlitz believes the intent is to clarify that “access points” to an ESP can be effectively moved with the application of appropriate equipment. A communication link between two ESPs utilizing an encrypted tunnel must have an encryption/decryption device at each end inside the ESP, this is defined as the “termination point”. However, if an additional protective device is added before the “termination point” to protect the ESP, would this not affectively move the “access point?” Must the logs of both protective devices be maintained?
Response3: Thank you for your comment. The drafting team could not be more prescriptive given the language in the standard. While it is true that the design and architecture will determine the endpoints, providing specific examples may unintentionally lead to perceived additional requirements that do not exist in the standard. In regard to your second comment, the insertion of an additional protective device ahead of the tunnel endpoint does not necessarily make that device an access				

<table>
<tr><th>Voter</th><th>Entity</th><th>Segment</th><th>Vote</th><th>Comment</th></tr>
<tr><td colspan="5">point for purposes of the tunneled traffic because it cannot enforce access control and monitoring for the contents of that tunnel; it depends also on any other functions the protective device is performing. It may still be considered an access point for the ESP depending on the design and architecture.</td></tr>
<tr><td>Mark Alberter</td><td>Sacramento Municipal Utility District</td><td>3</td><td>Negative</td><td>Further clarification for Q2: Is the communication link physical or logical? Where does it begin and terminate? is required. Specific guidelines identifying the physical or logical links should be identified.</td></tr>
<tr><td colspan="5"><b>Response4:</b> Thank you for your comment. The drafting team interprets that the communication links could be either physical or logical and whether their endpoints are access points or not depends on the design and architecture.</td></tr>
<tr><td>Michael Gammon</td><td>Kansas City Power & Light Co.</td><td>1</td><td>Negative</td><td rowspan="3">It is difficult or impossible to determine if a control is equivalent or better than a completely enclosed six wall border. This interpretation creates more ambiguity in the standard.</td></tr>
<tr><td>Charles Locke</td><td>Kansas City Power & Light Co.</td><td>3</td><td>Negative</td></tr>
<tr><td>Thomas Saitta</td><td>Kansas City Power & Light Co.</td><td>6</td><td>Negative</td></tr>
<tr><td colspan="5"><b>Response5:</b> Thank you for your comment. This comment may have been intended for the PacifiCorp request for an interpretation of CIP-006 (Project 2009-13).</td></tr>
<tr><td>Scott Heidtbrink</td><td>Kansas City Power & Light Co.</td><td>5</td><td>Negative</td><td>not clear if a control is equiv or better than a 6 wall border</td></tr>
<tr><td colspan="5"><b>Response6:</b> Thank you for your comment. This comment may have been intended for the PacifiCorp request for an interpretation of CIP-006 (Project 2009-13).</td></tr>
</table>

<table>
<tr><th>Voter</th><th>Entity</th><th>Segment</th><th>Vote</th><th>Comment</th></tr>
<tr><td>Tom Bowe</td><td>PJM Interconnection, L.L.C.</td><td>2</td><td>Negative</td><td>o In response to Q1: PJM has no concerns over this interpretation. o In response to Q2: PJM has no comments. This question and its answer are vague. o In response to Q3: PJM does not have concerns about this response as far as it refers to physical communication link termination; however, with regard to logical communication links, this could be taken to mean that any device at which a logical connection into the ESP terminates, would be considered an access point. PJM disagrees with this interpretation. o In response to Q4: PJM disagrees with this interpretation. VPN traffic should not be considered as different from any other logical connection. The access point to the ESP is able to provide layer 3 and 4 protection regardless of the type of traffic that is being traversed.</td></tr>
<tr><td colspan="5"><b>Response7:</b> Thank you for your comments. The drafting team interprets a communication link that originates from outside of the ESP and terminates within or at the ESP is an access point (physical or logical).
An encrypted tunnel that originates from outside of the ESP and terminates within or at the ESP is an access point. The drafting team offers that encrypted data cannot be adequately inspected at an upstream access point, such as a firewall, in order to provide the required level of protection. Therefore, the termination point must be considered an access point to the ESP and must be protected per CIP-005.</td></tr>
<tr><td>Robert Smith</td><td>Duke Energy</td><td>5</td><td>Negative</td><td rowspan="3">Per the response provided by the Cyber Security Order 706 SAR Drafting team to Question #4, in such instance where a Layer 3 encryption tunnel is deployed between two NERC CIP ESPs (electronic security perimeters), the termination points of such tunnels would need to be considered “access points” and thus NERC CIP requirement CIP 005 R2 would apply in its entirety to these termination points. A distinction has to be made in the response in regards to the encryption tunnel termination point when deciding whether such termination point is treated as an “access point” or not. 1. If a tunnel terminates in front of a Layer 3 filtering device and the traffic is passed through the Layer 3 filtering device in clear text, then the Layer 3 filtering device should be regarded as an “access point” as opposed to the encryption tunnel’s termination point being an “access point”. In this case the Layer 3 filtering device is capable of performing its access control function and is not processing any encrypted data. 2. If a tunnel terminates after passing encrypted traffic through a Layer 3 filtering device, then the Layer 3 filtering device’s capability of data traffic filtering is severely reduced and therefore the tunnel termination point should be treated as an “access point”.</td></tr>
<tr><td>Douglas E. Hils</td><td>Duke Energy Carolina</td><td>1</td><td>Negative</td></tr>
<tr><td>Henry Ernst-Jr</td><td>Duke Energy Carolina</td><td>3</td><td>Negative</td></tr>
<tr><td colspan="5"><b>Response8:</b> Thank you for your comment. The drafting team agrees with your comment that the termination point in your first example is not an access point. Subsequent clarification from PacifiCorp indicated that the tunnel terminated inside the ESP.
In regard to your second example, the drafting team again agrees with you. The insertion of an additional protective device ahead of the tunnel endpoint does not</td></tr>
</table>

<table>
<tr><th>Voter</th><th>Entity</th><th>Segment</th><th>Vote</th><th>Comment</th></tr>
<tr><td colspan="5">necessarily make that device an access point for purposes of the tunneled traffic because it cannot enforce access control and monitoring for the contents of that tunnel; it depends also on any other functions the protective device is performing. It may still be considered an access point for the ESP depending on the design and architecture.</td></tr>
<tr><td>Thomas J. Bradish</td><td>RRI Energy</td><td>5</td><td>Negative</td><td>RRI Energy votes negative in support of PacifiCorps position namely: 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. PacifiCorp recommends that entities not support this provided interpretation.</td></tr>
<tr><td colspan="5"><b>Response9:</b> Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication. The drafting team consulted with PacifiCorp in order to understand the specific details of its concern, and we believe the interpretation of the standard addresses PacifiCorp's specific situation.</td></tr>
<tr><td>Robert Kondziolka</td><td>Salt River Project</td><td>1</td><td>Negative</td><td rowspan="4">SRP has specific concerns with the answer to question 4 within the Interpretation. The Firewall access points already enforce port/protocol restrictions which meet the requirement. Adding the further restriction of access points at the encryption endpoint is unnecessary, increases complexity which by definition reduces reliability, and can have much wider implications beyond encrypted tunnels.</td></tr>
<tr><td>John T. Underhill</td><td>Salt River Project</td><td>3</td><td>Negative</td></tr>
<tr><td>Glen Reeves</td><td>Salt River Project</td><td>5</td><td>Negative</td></tr>
<tr><td>Mike Hummel</td><td>Salt River Project</td><td>6</td><td>Negative</td></tr>
<tr><td colspan="5"><b>Response10:</b> Thank you for your comment. The firewall access point ahead of the tunnel endpoint does not make that upstream device an access point because it cannot enforce access control and monitoring for the contents of that tunnel. Terminating the tunnel immediately before the firewall would allow the firewall to provide the required level of access control and monitoring and would not increase complexity.</td></tr>
<tr><td>Marcus V Lotto</td><td>Southern California Edison Co.</td><td>6</td><td>Negative</td><td>The concern with the Proj. 2009-12 interpretation is the 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.</td></tr>
<tr><td colspan="5"><b>Response11:</b> Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint,</td></tr>
</table>

Voter	Entity	Segment	Vote	Comment
irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.				
Fred E. Young	Northern California Power Agency	4	Negative	The interpretation does not provide any additional clarity.
Response12: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.				
Ray Mammarella	PP&L, Inc.	1	Negative	The interpretation provides minimal clarification based on the questions posed, including prior, similar requests for interpretation. This raises more questions in a complex area where many entities seem to be looking for clear definition and differentiation of terms such as access points and endpoints for their specific, varied, and arguably secure, network design/architectural configurations. For example in the response to Question 4 there is discussion relative to Layers 3 and higher, but there is nothing said for Layer 1 or 2.
Mark A. Heimbach	PPL Generation LLC	5	Negative	
Response13: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication. In response to latter part of your comment, tunnels that are layer 1 or 2 effectively create a single ESP.				
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	The Interpretation with respect to Question 4, implies that use of encryption is not suitable means of protection for access. If an encrypted tunnel is used between two ESP's, it would appear that the encryption itself would ensure restricted access and therefore any aspect of the communication would be secure.
Response14: Thank you for your comment. The interpretation does not imply that encryption is inadequate to provide some level of protection for access. The interpretation clarifies that endpoints, on or inside an ESP, to an encrypted tunnel that originates from outside of an ESP are access points and are subject to CIP-005.				
Gregory L. Pieper	Xcel Energy, Inc.	1	Negative	The language in response to question 2 does not provide any clarity as to what constitutes a communication link's termination points.
David F.	Xcel Energy,	6	Negative	

<table>
<tr><th>Voter</th><th>Entity</th><th>Segment</th><th>Vote</th><th>Comment</th></tr>
<tr><td>Lemmons</td><td>Inc.</td><td></td><td></td><td></td></tr>
<tr><td>Michael Ibold</td><td>Xcel Energy, Inc.</td><td>3</td><td>Negative</td><td>See Xcel Energy Transmission comments.</td></tr>
<tr><td colspan="5"><b>Response15:</b> Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</td></tr>
<tr><td>David Schiada</td><td>Southern California Edison Co.</td><td>3</td><td>Negative</td><td>The proposed interpretation does not provide sufficient clarity around the characteristics of an “endpoint” and what devices are in scope as being associated with “data communication links”.</td></tr>
<tr><td colspan="5"><b>Response16:</b> Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The drafting team interprets that either physical or logical data communications links are included and whether their endpoints are access points or not depends on the design and architecture.</td></tr>
<tr><td>Terry Harbour</td><td>MidAmerican Energy Co.</td><td>1</td><td>Negative</td><td>The proposed interpretation provides no meaningful clarity.</td></tr>
<tr><td colspan="5"><b>Response17:</b> Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.</td></tr>
<tr><td>James R. Nickel</td><td>Michigan Public Power Agency</td><td>5</td><td>Affirmative</td><td>As written, the response is appropriate. However, MPPA suggests that two distinct ESP's owned by a single entity and connected by a secured VPN should be considered a single ESP. This issue should be revisited by the Standards Drafting Team during writing of the Version 3 Standards.</td></tr>
<tr><td colspan="5"><b>Response18:</b> Thank you for your comment. The drafting team agrees with your suggestion and offers that such a topology can be considered a single ESP under the current version of this standard.</td></tr>
<tr><td>Guy V. Zito</td><td>Northeast Power Coordinating Council, Inc.</td><td>10</td><td>Affirmative</td><td>Further clarification should be pursued either through a future revision of the standard or a SAR specificall for the last sentence “Devices controlling access into the Electronic Security Perimeter are not exempt.” Suggest removing or replacing with “Devices controlling access into the Electronic Security Perimeter must comply with the Standards, as described in CIP-005 R1.5</td></tr>
</table>

Voter	Entity	Segment	Vote	Comment
Response19: Thank you for your comment and suggestion. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments be directed to that drafting team.				
Stanley M Jaskot	Entergy Corporation	5	Affirmative	Need a definition of "encrypted tunnel"
Response20: Thank you for your comment. The drafting team acknowledges your suggestion for a definition of “encrypted tunnel” however the scope of our work is limited to interpreting the existing standard. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments, including the proposed new NERC *Glossary of Terms Used in Reliability Standards* definition, be directed to that drafting team.				
Peter T Yost	Consolidated Edison Co. of New York	3	Affirmative	Regarding the CIP-005 Interpretation, the following comment is submitted: "Further clarification should be pursued either through a future revision of the standard or a SAR specifically for the last sentence "Devices controlling access into the Electronic Security Perimeter are not exempt." Suggest removing or replacing with "Devices controlling access into the Electronic Security Perimeter must comply with the Standards, as described in CIP-005 R1.5."
Response21: Thank you for your comment and suggestion. There is revision work currently being conducted on standards CIP-002 through CIP-009 under Project 2008-06: Cyber Security Order 706. We suggest that your comments be directed to that drafting team.				
Ronald D. Schellberg	Idaho Power Company	1	Abstain	Interpretation does not aid in the interpretation of the standard.
Response22: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.				
Jerome Murray	Oregon Public Utility Commission	9	Abstain	Our concern is the 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.
Response23: Thank you for your comment. The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The drafting team interprets that either physical or logical data communications links are included and whether their endpoints are access points or not depends on the design and architecture.				