NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Initial Ballot — CIP-006-1 — Progress Energy Request for Interpretation (Project 2008-10)

Summary Consideration: There are five themes that emerged from the industry comments:

1) Wiring does not rely upon or utilize a routable protocol and thus cannot be a cyber asset any more than a power cable is. The NERC definition of cyber asset does not include the language "including the wiring that comprises the physical media supporting the network."

Response: The interpretation response team has reviewed its response and considers the wiring to be a component of the communication network, which is a cyber asset, as defined in the NERC Glossary. As such, the network wiring needs to be protected.

2) This is far too important to resolve via an interpretation. This needs to be addressed in the revisions to the CIP standards and subject to the full stakeholder process.

Response: We agree that this is an important issue, and it will be considered as part of the standards' revision in the Cyber Security Order 706 (CSO706) project (Project 2008-06). However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this request for interpretation (RFI) from Progress Energy.

3) The interpretation exceeds the process rules by changing the requirements of standard, adds concepts not consistent with other NERC guidance, speculates on the intent of the standard, and adds confusion and ambiguity with respect to compliance. It also opens the door for other non-physical "alternatives" to compliance with the requirements of CIP-006.

Response: While the drafting team disagrees it altered any requirements to the standard via the interpretation, the team acknowledges a lack of clarity regarding alternative measures. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection for Electronic Security Perimeter (ESP) wiring that is external to the Physical Security Perimeter (PSP).

4) The wire is not within the ESP; therefore it does not need to be protected. The wire is nothing more than a communication link specifically excluded by CIP-005, R1.3.

Response: The request clearly asked about wiring within an ESP.

5) The cost (dollars, time) to protect wiring in a campus setting far exceeds the benefit derived by doing so. The challenges of having to comply with all of the CIP-006 requirements are an impossible and unreasonable task. The decision to protect wiring should be based upon a proper risk determination process.

Response: The interpretation response team attempted to offer alternative methods for compliance without undue financial burden in the initial interpretation response. In drafting the revised interpretation, the team interprets the phrase "alternative measures" to include use of combined/complementary physical and logical approaches to achieve the same or better protection.

Entity	Segment	Vote	Comment
Allegheny Power	1	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information

Entity	Segment	Vote	Comment
			transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: 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. 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. 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. The RFI response drafting team agrees that this is an important issue and it will be considered as part of the standards’ revision in the Cyber Security Order 706 (CSO706) project.			
Ameren Services Company	1	Negative	We do not agree with this interpretation. We feel that the language in the first sentence of the response, "including the wiring that comprises the physical media supporting the network," could be viewed to include aspects that are not covered in the CIP 002 - 009. Broad interpretation of the response would significantly impact the compliance burden. In addition, 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." This interpretation does not make it clear whether or not that part of the CIP-006 requirement 006 is still valid, and seems to supersede the CIP standard in this regard.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within			

Entity	Segment	Vote	Comment
an ESP, but the wiring itself is not a separate Cyber Asset. 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.			
American Electric Power	1	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being considered as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A methodology for determining the appropriate protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. 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.			
Associated Electric	1	Negative	Wiring meets none of the requirements of CIP-002-R3, the wiring does not communicate itself with anything, it is merely a communications conduit or channel, therefore the standard does not apply to it anymore than it

Entity	Segment	Vote	Comment
Cooperative, Inc.			would apply to the ac power wiring. While it is appropriate to protect access to all wiring inside the ESP, I do not believe that the intent of the standard is to consider wiring a CCA and subject it to all of the CIP requirements, many of which can not even be implemented or do not apply. These points were presented very well (and I am in complete agreement with) in the document by Mr. Tim Conway of NiSource, “Wiring as a CCA”.
Response: 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. 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.			
Brazos Electric Power Cooperative, Inc.	1	Negative	Further clarity should be added to the last sentence to address the interpretation request as follows: Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures as it extends from the ESP up to the Physical Security Perimeter. Then there is the question about what is defined as "tampering".
Response: 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. 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. 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. The RFI response drafting team views tampering to include, but is not limited to, unauthorized access, disruption, or alteration.			
Consolidated Edison Co. of New York	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.

Entity	Segment	Vote	Comment
Response: 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. 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 and logical approach to achieve the same or better protection. 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.			
FirstEnergy Energy Delivery	1	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that "Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: 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. The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The communication assets excluded from the standards are the Cyber Assets associated with communication networks and data communication links between			

Entity	Segment	Vote	Comment
discrete ESPs. There is no explicit reference within the standards to third-party communications. 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.			
Hydro One Networks, Inc.	1	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: The equipment configuration described in this comment wherein two physically separate Cyber Assets that are individually classified as having its own ESP would indeed not require physical access protection for the interconnecting wiring. However, the situation as described by the requestor is different. The configuration indicated by the requestor involves physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	1	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that “the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network.” It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised RFI response. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the			

Entity	Segment	Vote	Comment
drafting team disagrees with removal of the term communication network in the RFI response as it is already referenced in the NERC Glossary definition of a Critical Cyber Asset.			
National Grid	1	Negative	The interpretation is not clear and may modify the intention of the Standard. The existing Standard requirement clearly states, "...all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. 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 for ESP wiring that is external to the PSP 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.			
New Brunswick Power Transmission Corporation	1	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "…all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset 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 and logical approach to achieve the same or better protection. 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.			
Orange and Rockland Utilities, Inc.	1	Negative	Orange and Rockland cannot support CIP-006 R1.1 and requests further clarification of "alternative protection measures" encompassing the wiring that comprises the "physical media" supporting the network.
Response: 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 for ESP wiring that is external to the PSP may include, but are not			

Entity	Segment	Vote	Comment
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.			
Pacific Gas and Electric Company	1	Negative	As written the interpretation is too broad. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within the pertinent parts of a given facility or campus.
Response: 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 for ESP wiring that is external to the PSP 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.			
PacifiCorp	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: 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. 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. The drafting team believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected not to include such language.			
Potomac Electric	1	Negative	Pepco is a subsidiary of PHI. PHI feels that the interpretation is not clear and the response itself is subject to interpretation. This lack of clarity is the basis for PHI's rejection. PHI also believes that communication systems

Entity	Segment	Vote	Comment
Power Co.			should be protected. The Answer to Question 11 of the FAQ associated with these standards states that communication systems are not covered by these standards.

Response:

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. The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

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.

Question 11 of the FAQ for standard CIP-002-1 – Cyber Security – Critical Cyber Assets (reproduced below) refers to Section A 4.2.2 regarding the exclusion of Cyber Assets associated with communication networks and data communication links between discrete ESPs. Communications within the ESP are covered by these standards.

CIP-006-1 The asset owner is encouraged to reconsider the design of a communication network that extends the ESP across third-party communications systems and networks.

11. FAQ - Question: *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?*

Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.

PP&L, Inc.	1	Negative	The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.

Response:

The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.

Entity	Segment	Vote	Comment
Puget Sound Energy, Inc.	1	Negative	Definition of Cyber Asset: We do not believe the existing definition of "Cyber Asset" should include wiring. From the most recent (February 12, 2008) NERC "Glossary of Terms Used in Reliability Standards": "Cyber Assets - Programmable electronic devices and communication networks including hardware, software, and data." Wires are not programmable, are not software, and are not data. While they are physical media, it is highly questionable if they could be considered hardware as our understanding is that hardware devices are what software runs on. If we were to extend the definition to include a wire strictly because it carries data, at what point do we consider a telephone pole a Cyber Asset because it carries wires which carry data? If the definition does include wiring, how then do wireless communications media fit into the definition in the context of physical protection of Cyber Assets? Wireless is neither hardware, software, or data and, with regards to this interpretation, physical protection of airborne electrons is not practical/possible with today's technology. Alternative Protective Measures: As most facilities which house Critical Cyber Assets were constructed prior to the CIP standard adoption by FERC, many such facilities have a common wiring infrastructure for both Critical Cyber Assets and assets that are not in scope for CIP compliance. We believe it is unreasonable to require every wire be traced and extracted from common conduit, cable bundles, or other common pathway for the purposes of re-enclosing them in a CIP-specific conduit or other “six-wall” perimeter. The very act of performing this work will introduce an increased reliability risk. If wiring is to be included in the definition of Cyber Asset, we feel that a “completely enclosed (“six-wall”) border” cannot be established for most wiring infrastructures given the above. Therefore, the "alternative measures to control physical access to the Critical Cyber Assets" phrase from CIP-006 R1.1 must be used. The definition for Critical Cyber Assets require that a Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, the Cyber Asset uses a routable protocol within a control center; or, the Cyber Asset is dial-up accessible, and wiring has no such attributes. Given that CIP-006 R1.1 talks about both Cyber Assets and Critical Cyber Assets, can the interpretation team comment on the above? We would also like clarification on whether "alternative protective measures" includes situations that only deploy purely logical controls of data transiting the wire. As the interpretation team has stated, “The intent is to protect the data transmitted over the network within the ESP”, would an ESP that spans an entity’s entire infrastructure and only employs logical “alternative protective measures”, be an acceptable response to this interpretation? Summary: We commend the interpretation team for wanting to address data in motion, but the appropriate venue to address this issue is NERC Project 2008-06 as CIP-006 R1.1 prescribes requirements for physical protection of Cyber Assets (or just Critical Cyber Assets when a “six-wall” perimeter cannot be established) within an ESP. Additionally, based on our assessment of the term Cyber Asset, we believe requirements to protect communications media are beyond the scope of the existing CIPs. Outstanding RFI How does the Project 2008-10 interpretation for Progress Energy relate to the previous interpretation request (below) from October 10, 2007 by Puget Sound Energy? --- 1) We are requesting an interpretation of the term “externally connected” as used in 005.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) We request an interpretation which allows encrypted connections over frame relay within a single ESP. Note in the diagram above the routers are not considered “access points” to the ESP, but rather are contained within it. 2) We are requesting clarification of CIP-006-1 R1.1: Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely

Entity	Segment	Vote	Comment
			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 standard does not explicitly require a given ESP to be fully contained by a single PSP. We request a clarifying interpretation which allows an ESP to span multiple PSPs provided that communications within the ESP are protected sufficiently to prevent unauthorized access. Commentary: With the use of encrypted tunnels and physical protection of the tunnel endpoints, we believe that secure, CIPS compliant ESPs can be designed which span multiple PSPs. It should be noted that 005.R1.3 defines communication links between ESPs as an "access point", which in turn requires port/protocol restrictions at the access point (005.R2.2). However, OSI layer 3 controls won't solve what is fundamentally an OSI layer 2 concern. Specifically, port and protocol restrictions at the endpoints of a frame relay connection will not adequately mitigate the risk of exposure to packets being manipulated at OSI Layer 2. Hence, our desire to use encrypted tunnels to assure packet integrity and source authenticity thereby addressing the layer 2 concerns. Thank you for the opportunity to comment.
Response: The RFI response team agrees with the comment that the main objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. In regard to wiring, the RFI response drafting team asserts that the definition of Cyber Asset in the NERC Glossary indeed includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. With respect to the commentary about a single ESP spanning multiple PSPs, the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies. The drafting team is not familiar with the October 10, 2007 RFI by Puget Sound Energy.			
Salt River Project	1	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response:			

Entity	Segment	Vote	Comment
The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	1	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.

Response:

The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.

The scenario described in this comment wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring.

The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection.

The recommendation to address data in motion is currently included in the work of the CSO706 Project.

Entity	Segment	Vote	Comment
Sierra Pacific Power Co.	1	Negative	This interpretation seems to expand the applicability of the CIP Requirements outside the bounds of the Critical Assets.
Response: The RFI response drafting team does not expand the applicability of the CIP requirements but states the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Southern California Edison Co.	1	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team's proposed interpretation for CIP-006-1's Requirement 1.1 ("Proposed Interpretation"). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that "Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rites dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that			

Entity	Segment	Vote	Comment
is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, the request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Southern Company Services, Inc.	1	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase "alternative measures" in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Southwest Transmission Cooperative, Inc.	1	Negative	"The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response:			

Entity	Segment	Vote	Comment
The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team believes alternative measures is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible.			
Tampa Electric Co.	1	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security “ such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Entity	Segment	Vote	Comment
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	1	Negative	While we agree that physical and electronic perimeters must be the same or the data must protected as it traverses physical perimeters, TVA doesn't think that the interpretation provides sufficient detail to guide compliance.
Response: The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team is limited in its ability to provide more explicit guidance and believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tucson Electric Power Co.	1	Negative	TEP supports the following provided by WECC: "The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus." "If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances."
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to			

Entity	Segment	Vote	Comment
avoid such language.			
Westar Energy	1	Negative	Disagree with the concept that wire is a Cyber Asset.
Response: The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			
Western Area Power Administration	1	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Xcel Energy, Inc.	1	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on

Entity	Segment	Vote	Comment
			entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription such as in a diagram but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
British Columbia Transmission Corporation	2	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California ISO	2	Negative	The interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with “what should have been done”. The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, R1.1 "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. 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." CIP-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Glossary: "Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Independent Electricity System Operator	2	Negative	Although directionally the IESO is in favour of the intent of the interpretation, we believe the current interpretation wording may effectively modify the intention of the standard, which is inconsistent with NERC standard development protocol, and hence the interpretation needs more work. CIP-006-1, R1.1 states: "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures TO CONTROL PHYSICAL ACCESS(emphasis added) to the Critical Cyber Assets." the interpretation states: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring OR ALTERNATIVE PROTECTIVE MEASURES(emphasis added). Whereas the standard clearly requires physical access control, the interpretation effectively relaxes this requirement with the words either through physical protection of the wiring or alternate protective measures where the resultant implication is that the alternate protective measures are non-physical, hence a relaxation of the standard. Although we believe the standard should be revised to allow alternative protective measures, that is not the issue being balloted.
Response: The RFI response drafting team respectfully disagrees that the scope of alternative measures does not include logical approaches. The drafting team concurs that the intent is to protect the data that travels over the wiring and asserts that either physical or logical measures are capable of achieving the desired objective.			
ISO New England, Inc.	2	Negative	There are three significant issues with this Interpretation which resulted in a negative vote: (1) the interpretation adds requirements that are not already part of the Standard, the Standard intentionally did not originally address data in transit over communication links; (2)the interpretation creates conflicts between CIP-006 R1.1 and CIP-005, R1.3, which clearly states that communication links connecting discrete ESPs shall not be considered part of the ESP; and (3) we believe that the current Standard is clear enough and this interpretation simply creates more confusion in the industry, we have not had any problems in understanding or implementing

Entity	Segment	Vote	Comment
			the Requirements in this Standard.
Response: (1) The notion of data in transit, while at the core of the protection purpose, is more appropriately addressed in the ongoing CSO706 Project. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. (2) Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. (3) The drafting team is compelled by process to respond to this RFI from Progress Energy.			
Midwest ISO, Inc.	2	Negative	The FAQ developed along with the original CIP standards specifically state that the standards are not intended to address the wires between facilities. While we agree that the suggested interpretation is a good idea for a future improvement to the standard, the interpretation process is intended to clarify what the standard says as originally drafted, not what we would like the standard to say.
Response: The FAQ is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity, such as third party telecommunications company equipment. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. In this instance, the wiring referenced by Progress Energy is clearly within a single ESP. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.			
PJM Interconnection, L.L.C.	2	Negative	PJM has the following concerns: Procedural: the interpretation adds requirements that are not already part of the standard. CIP-006-1 describes the requirements for physical access controls. An interpretation of a standard should not be confused with "what should have been done". The NERC Standards development process says that an interpretation cannot modify a standard, only clarify its meaning. By including an explicit reference to data in transit over communications links between discrete perimeters, the interpretation moves into an area which the standard intentionally does not address. Conflicts: the interpretation crosses multiple standards CIP-006-1, R1.1 "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. 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." CIP-005-1, R1.3: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Glossary: "Cyber Assets: Programmable

Entity	Segment	Vote	Comment
			electronic devices and communication networks including hardware, software, and data." The reference in CIP-005, R1.3 describes "communication links"; in reality, those links are the "wiring" that the interpretation request is describing; thus, they are not within the Electronic Security Perimeter and do not need to be within a Physical Security perimeter. Necessity: the definitions and descriptions contained within the published standard seem clear; the issue has posed no significant problems for SWG member organizations to understand or implement.
Response: The RFI response drafting team recognizes that while data in transit is fundamentally the asset to be protected, it agrees that the CSO706 Project is where it should be addressed. This interpretation does not add a requirement to protect communication links, or the data transiting thereon, that are outside of the ESP. The definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Alabama Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
American Electric Power	3	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively

Entity	Segment	Vote	Comment
			accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	3	Negative	The interpretation is not clear, may modify the intention of the Standard, and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: 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. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	3	Negative	Consumers Energy’s understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America’s control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control

Entity	Segment	Vote	Comment
			and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to any externally connected communication end point (for example, dial-up modems) as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.
Response: The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a			

Entity	Segment	Vote	Comment
single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. 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. Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP. The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Cowlitz County PUD	3	Negative	Cowlitz County PUD No.1 (District) finds the interpretation does not clarify the intent of the Standard. Extension of the "6-wall" physical security perimeter with conduit would require an accounting for all access points (condulets or conduit bodies) and appropriate access monitoring. Simple use of conduit does not offer the best protection of data as it can be easily compromised. The verbiage "or alternative protective measures" needs clarification - or alternative physical and/or logical protective measures - to protect the original intent of the Standard. The District's position is that logical protective measures (such as loss of continuity alarms) will in many cases better protect data from malicious tampering than physical protective measures.
Response: The RFI response drafting team clarifies CIP-006 R1.1 which 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 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 or monitoring for circuit disruptions due to physical tampering.			
Duke Energy Carolina	3	Negative	Thank you for the opportunity to vote on this interpretation. We think that the interpretation is unclear. A new NERC Cyber Security drafting team is in the process of being assembled, and Duke Energy believes that this issue is best addressed in a comprehensive manner by the new Cyber Security drafting team. The manner of protecting data from tampering when it is transmitted over networks should be clearly defined in the new Cyber Security Standard, and any newly prescribed protection methods must be properly related to other requirements in the standards where that is appropriate.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			

Entity	Segment	Vote	Comment
FirstEnergy Solutions	3	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that ""Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and 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 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 or monitoring for circuit disruptions due to physical tampering.			
Georgia Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. -

Entity	Segment	Vote	Comment
			The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Gulf Power Company	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. The RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-2 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
Hydro One Networks, Inc.	3	Negative	Hydro One Networks Inc. is casting a Negative vote with the following comment: The interpretation is not clear and may modify the intention of the Standard. It needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter," which must be protected. While the wires connecting two ESPs need to be protected it should not make one PSP of both. Appropriate conduit or similar protection as appropriate should be acceptable.
Response: 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. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the			

Entity	Segment	Vote	Comment
connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. Appropriate conduit, as suggested by the commenter, is an acceptable physical protection.			
Lincoln Electric System	3	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 applies.			
Madison Gas and Electric Co.	3	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the

Entity	Segment	Vote	Comment
			explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal Interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. 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. The RFI response drafting team disagrees with the commenter that the exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are 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 or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	3	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.			

Entity	Segment	Vote	Comment
However, the drafting team disagrees with removal of the term communication network in the RFI response as it already referenced in the NERC Glossary.			
MidAmerican Energy Co.	3	Negative	MidAmerican Energy believes that this interpretation expands the requirements of the standard inappropriately.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
Mississippi Power	3	Negative	- The interpretation is not supported in any way by the wording of the standard; it actually represents an extension of the standards without sufficient discussion within the industry or comparison to acknowledged industry best practice. - The interpretation was written by a body, the CIP version 2 SAR drafting team, which was not formed for that purpose and which did not have specific expertise to be able to address the problem. - The interpretation creates a number of unresolved issues by using vague language around alternate measures. - The interpretation creates a situation where a CCA may need to be identified which can only be subject to one of the many requirements in the standards and which makes it difficult to reconcile the status of a cable or wireless CCA with the language of the other standards.
Response: The RFI response drafting team is asked to interpret the wording in a standard. 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. The phrase “alternative measures” in the Requirement R1.1 of CIP-006-1 is interpreted by the drafting team to include physical and logical protection approaches. The team is comprised of industry subject matter experts in the field of cyber security.			
New York Power Authority	3	Negative	The interpretation is not clear and may modify the intention of the Standard, in our opinion, and needs more work. The existing Standard requirement clearly states, "... all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: 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. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a			

Entity	Segment	Vote	Comment
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 or monitoring for circuit disruptions due to physical tampering.			
Niagara Mohawk (National Grid Company)	3	Negative	The interpretation is not clear and may modify the intention of the Standard and therefore needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimieter", which must be protected.
Response: 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. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
Platte River Power Authority	3	Negative	The interpretation would be acceptable if language is added similar to what is suggested below: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering. Where (“six-wall”) physical protection of the wiring cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Response: 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. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to			

Entity	Segment	Vote	Comment
physical tampering.			
Public Utility District No. 2 of Grant County	3	Affirmative	
Salt River Project	3	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat.
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Seattle City Light	3	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			

Entity	Segment	Vote	Comment
The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			
Tampa Electric Co.	3	Negative	Tampa Electric Company’s Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry’s attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective

Entity	Segment	Vote	Comment
			based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. • Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
Wisconsin Public Service Corp.	3	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website. Standard CIP-002-1 — Cyber Security — Critical Cyber Assets 11. Question: Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards? Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. Standard CIP-005-1 Cyber Security — Electronic Security 2. Question: I am connected to other partners Electronic Security Perimeters through a Wide Area Network (WAN) connection. What is now included in the Electronic Security Perimeter? Is the connection to the partner included? Answer: The standard states that where discrete Electronic Security Perimeters are connected by communication lines, the communication lines are not included in the Electronic Security Perimeter. 15. Question: Is a physically isolated and dedicated network required for connections between Electronic Security Perimeters? Answer: No, physical isolation is not required, nor is a dedicated link required. The standard does not specify any requirement for communication between discrete Electronic Security Perimeters, since this is currently beyond the scope of these standards. It

Entity	Segment	Vote	Comment
			is possible for the data between discrete perimeters to be carried over a shared infrastructure such as a shared WAN, or to be carried over dedicated links. However, the Responsible Entity must ensure that the access control devices (such as firewalls) at the access points to the Electronic Security Perimeters do not permit unauthorized access to the Electronic Security Perimeters and the Cyber Assets within them. When data is carried over a shared infrastructure, the Responsible Entity should ensure as well that the data has not been changed in transit. Logical or virtual separation of the data in a shared infrastructure can be accomplished by using existing technologies such as virtual circuits and communication tunnels. Encryption or other data integrity checking technologies can also ensure that data is not changed in transit, provided performance and latency requirements for the applications are satisfied. Standard CIP-006-1 — Cyber Security — Physical Security 20. Question: Does the standard require entities to protect telecommunications services and facilities that serve physical security system assets? Answer: CIP-002 through CIP-009 do not address telecommunications.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. The RFI response team clarifies in a revised interpretation response that physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. Protection of communication systems that reside within an ESP is required. The Frequently Asked Questions posted on the NERC website is a guidance document and is not mandatory and enforceable as NERC standards are. However, question #11 (reproduced below) refers to assets that are not owned by the Responsible Entity such as third-party telecommunications company equipment. **11. FAQ - Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?* **Answer:** Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset. In addition, the figure associated with Question 2 for CIP-005-1 (Page 12 of the FAQ) specifically addresses the commenter's concerns regarding interconnectivity of ESP's over Wide Area Networks. This interpretation does not change the exclusion of communication networks outside of an ESP from the standard. In this instance the wiring is clearly stated by Progress Energy to be within a single ESP.			
Xcel Energy, Inc.	3	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these

Entity	Segment	Vote	Comment
			rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Alliant Energy Corp. Services, Inc.	4	Negative	CIP-005 - R1.3 specifically excludes the connecting cabling from the CIP standards. There can not be such conflicting statements between standards.
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Consumers Energy	4	Negative	Consumers Energy's understanding of the requirements of CIPS-005-1 and CIPS-006-1 as they were being developed and as they exist today allowed for discrete non-contiguous physical security perimeters to protect cyber assets contained within a single electronic security perimeter, presumably by excluding the communication network and data passing over the communication network as being defined as Cyber Assets requiring physical protection. We believe that this view is consistent with good utility practice utilized at a number of North America's control centers and generating plants. In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the original drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems or devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, and none of the nine requirements specifically address network cables or data. Had the original intent of the standards been to include the communication networks within an electronic security perimeter as Cyber Assets requiring physical protection we would have expected the standard to address appropriate protection where six-wall physical protection (complete with access control and monitoring) is not necessary (such as with buried portions of the network) or practical (such as within raceways or conduit). Additionally, the time required to re-wire such networks so as to provide six-wall physical protection is significantly longer than the time required to provide six-wall physical protection to the access points to Cyber Assets within the Electronic Security Perimeter. Further, had the original intent of the standards been to include data that passes over the communication network, the standard should have discussed the issues associated with transporting, storing and restoring back-up tapes and other removable media so as to protect cyber assets in the event the back-up data is re-introduced to the electronic security perimeter. We

Entity	Segment	Vote	Comment
			suggest the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. We believe the primary intent of the present version of the CIP Standards is to protect against remote compromise of those assets. The apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards as they were developed and implemented. CIP-006-1 R1.1 states "ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter." This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting communication network cabling residing in an area entirely within the reasonable and prudent control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all communication network and data as Cyber Assets requiring physical protection, the wording should have stated such. If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between "in-house" cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. We propose the following wording to replace the existing interpretation: Response: The Physical Security Perimeter is required to protect the access points to Critical Cyber Assets within the Electronic Security Perimeter. For dedicated communication networks within a discrete Electronic Security Perimeter under the normal reasonable and prudent control of the Responsible Entity, all elements of such network do not require to be contained within the Physical Security Perimeter so long as all access points to the Critical Cyber Assets within the Electronic Security Perimeter are also within a Physical Security Perimeter. CIP-005-1 R1.1 refers to " any externally connected communication end point (for example, dial-up modems) " as specifically identified as an access point to the Electronic Security Perimeter. The use of "externally connected" in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be "external" would include local area networks between floors in a building or between buildings in a campus environment.

Response:

The RFI response drafting team believes the commenter's presumption that protection is not required for wiring between "discrete non-contiguous physical security perimeters" is not justified. The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 justifiably applies.

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.

Although the drafting team is limited to respond to this request from Progress Energy, to the point about "communication links" cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.

Entity	Segment	Vote	Comment
The drafting team believes that the other concerns raised by the commenter, including transfer of backup tapes and other removable media, is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project.			
Madison Gas and Electric Co.	4	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. 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. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-			

Entity	Segment	Vote	Comment
006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are 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 or monitoring for circuit disruptions due to physical tampering.			
Seattle City Light	4	Negative	The reasoning for this vote is as follows: As noted in the Progress Energy submittal to NERC, they have cited the requirements for Critical Cyber Assets (CCAs) to be contained within the Electronic Security Perimeter (ESP) and for the ESP to be contained within the Physical Security Perimeter. However, a scenario can easily develop whereby CCA's are connected via cable/wiring and the affected wiring runs outside of the ESP and sometimes outside of the Physical Security Perimeter. In some instances the wiring could be underground, in cable trays, and even via poles and towers. Therefore, the key issue to recognize is that the cables/wires may be in circumstances whereby complete encapsulation (i.e., to achieve the "6-sided wall" mandate) would be extraordinarily expensive, extremely difficult, and in many cases not add any added physical protection due to the location of the wire/cable and distance away from unauthorized tampering. Also, if the cables are still within the physical security perimeter but outside the ESP, then added protection is not necessarily value added from a security standpoint because physical access is still afforded but not accepted in the interpretation. Our recommendation is that the interpretation take into account the security buffer between the Electronic Security Boundary and the Physical Security Boundary for cables/wires. Secondly, it is also recommended that protection of the data is paramount and that some logical controls should be taken into account for data protection even though the cable may be external to the ESP. Thirdly, encapsulating cable with conduit, cages or other "6-sided wall" protective measures may not be reasonable for the security value add and that the interpretation should take into account the physical location of the wires/cables that prevent an unauthorized party from tampering with the physical layer of the equipment.
Response: The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006. The scenario described by the commenter wherein two physically separate Cyber Assets that are individually classified as each having its own ESP would indeed not require physical access protection for the connective wiring. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. These measures can account for data protection. The recommendation to address data in motion is currently included in the work of the CSO706 Project.			

Entity	Segment	Vote	Comment
Seminole Electric Cooperative, Inc.	4	Negative	Seminole endorses the comments of Tampa Electric Company as replicated below: Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. We have several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach my be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment do not offer or support an approved mechanism for encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, we recommend that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.

Response:

The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.

Entity	Segment	Vote	Comment
However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Wisconsin Energy Corp.	4	Negative	Interpetation is overreaching
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
WPS Resources Corp.	4	Negative	The interpretation for CIP-006 significantly expands the scope of the standard and needs to go through through the SAR process. The inclusion of communications network wiring is a shift from previous industry understanding and is contrary to responses for Frequently Asked Questions posted on the NERC website.
Response: The RFI response drafting team does not expand the meaning of but rather interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
AEP Service Corp.	5	Negative	Although we agree that a true "systems" approach to data protection would also include the data paths, we are concerned about an element that we believe should be included in any determination of communication path physical security. Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or inobtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Allegheny Energy Supply Company, LLC	5	Negative	Allegheny Energy is concerned with the SAR drafting team interpretation that wiring within an ESP be considered a Cyber Asset or Critical Cyber Asset. Allegheny Energy agrees that the wiring (and information transmitted by such wiring) within an ESP needs to be protected; however, Allegheny Energy does not agree that the wiring needs to be classified and protected as a defined cyber asset. NERC defines cyber assets as programmable electronic devices and communication networks including hardware, software, and data and does not include the language “including the wiring that comprises the physical media supporting the network”. Allegheny Energy believes the best method to determine protection measures for the wiring (and information transmitted by such wiring) is to create a holistic approach to communication network and data communication link protection through the Standards process that specifically addresses these issues. This new Standard could address communication network and data communication link security issues, including copper cabling, fiber optic cabling, and wireless implementations. By the interpretation stating that network wiring is a cyber asset or potentially a critical cyber asset in an effort to physically secure the wiring, this statement would additionally impose all of the requirements of the CIP standard that are applicable to cyber assets and in essence make entities non-compliant since many requirements cannot be accomplished for wiring.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. As such the RFI response drafting team has clarified that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
City of Tallahassee	5	Negative	CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)."

Entity	Segment	Vote	Comment
			Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." I disagree that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
Colmac Clarion/Piney Creek LP	5	Affirmative	Appears to adequately require either 'six boundary' enclosure or entity description of protective measures on wiring or components outside of same. Doesn't require that entity methods equal six wall protection however.
Response: Thank you for your comment. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
Consumers Energy	5	Negative	Consumers Energy’s Comments to Accompany a “No” Vote on NERC 2008-10 August 6, 2008 **2008-10 Goes Beyond the Intent of the Standards** In extending the definition of Cyber Asset to include data and the communication network, the Interpretation clearly goes beyond the scope intended by the drafters of the Standards. CIP-002-1 R3, Critical Cyber Asset Identification, refers to several examples of possible Critical Cyber Assets, all of which can be considered computer systems, devices possessing a central processing unit. Seven of the nine requirements in CIP-007-1 refer to Cyber Assets and clearly are intended to apply to computer systems, not network cables or data. **Data and Cables Would Become Critical Cyber Assets** If this interpretation passes, network cables and data will be considered Cyber Assets. Since it is difficult to conceive of an Asset that uses a network where data and networks are not essential to the operation of that Asset, data and network cabling will become Critical Cyber Assets. This will be true for control centers, generating plants and substations. **Data as a Critical Cyber Asset** The act of identifying data as a Critical Cyber Asset has far-reaching implications. Will removable media such as backup tapes need to be stored within an Electronic Security Perimeter? How can media so protected be

Entity	Segment	Vote	Comment
			moved to an off-site storage location? **Actual Intent - Cyber Asset Has CPU** Consumers Energy suggests the actual intent of the CIP Standards is to define as a Cyber Asset only those devices with a central processing unit. These are the devices susceptible to remote attack and compromise. Consumers Energy further suggests the primary intent of the present version of the CIP Standards is to protect against remote compromise. **Intent of Interpretation Goes Too Far for This Stage** Consumers Energy also suggests that the apparent intent of the Interpretation, to require all network cabling be protected by a six-wall boundary, goes beyond the intent of the CIP Standards in their present form. CIP-006-1 R1.1 states “ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.” This does not require a piece of hardware without a CPU, such as a network cable, to reside within a six-wall boundary. Consumers Energy argues that protecting network cabling residing in an area entirely within the control of the Responsible Entity is beyond the scope of the present CIP Standards. Had the intent of the requirement been to include all connections outside the ESP, the wording should have stated such. Threats and Priorities If the apparent intent of the Interpretation, to require network cabling to be contained within a six-wall boundary, is accepted, there will be no distinction between “in-house” cabling and connections carried through public networks. This ignores the different threat exposure of the two types of communication circuits. This Interpretation will divert money and other resources from mitigating higher threat exposures, such as man-in-the-middle attacks on unencrypted external communications circuits, to this lower threat exposure. **Proposed Rewording** Consumers Energy proposes the following wording to replace the existing interpretation: Response: CIP-006-1 R1.1 refers to “any externally connected communication end point (for example, dial-up modems)” as specifically identified as an access point to the Electronic Security Perimeter. The use of “externally connected” in this context refers to communication facilities outside the control of the Responsible Entity. Examples of such connections would include dial-up or leased telephone or data circuits, commercial packet-switched networks, wireless networks, or the Internet. Examples of connections not considered to be ”external” would include local area networks between floors in a building or between buildings in a campus environment.

Response:

On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset.

The RFI response drafting team agrees and acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also notes that Critical Cyber Asset classification is an important issue and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. Therefore, the

Entity	Segment	Vote	Comment
matter of data protection is not directly address by this RFI response. The drafting team does not agree that protection of only Cyber Assets with CPUs is the intent of the CIP standards. The drafting team believes that the requirement clearly states that “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 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 or monitoring for circuit disruptions due to physical tampering. The RFI response drafting team appreciates the suggested replacement wording, but believes it does not meet the objective of CIP-006-1.			
Detroit Edison Company	5	Negative	The following are Detroit Edison's reasons for voting No: The NERC Glossary defines Cyber Assets as “Programmable electronic devices and communication networks including hardware, software, and data”. Detroit Edison believes that this definition relating to the network is to include active devices that comprise the network, not the transmission media itself. Thus routers, switches, hubs, etc. are cyber assets, wiring is not. Detroit Edison's opinion on protecting cabling between physical security perimeters fully contained within an otherwise adequately secured facility is that the cable is sufficiently protected following guidance provided by NIST. Additional protection can be provided by covering the cable trays where they are easily accessible. "NIST SP800-53 PE-4 Access Control For Transmission Medium, Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays." Note that conduit and cable tray is specified as adequate protection by NIST however, if the interpretation is approved as written a completely enclosed six wall boundary would be required. Does this mean that all conduit bodies, pull boxes, cable tray covers, and open cable trays would become access points subject to CIP-006? "FERC Order 706 paragraph 224: Congressional Representatives state that NIST research prepared a technical report comparing the proposed CIP Reliability Standards with SP 800-53. This technical report found that an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the CIP Reliability Standards, though the converse may not be true." Detroit Edison believes that the outer barrier cable jacket, designed and manufactured to protect the data transport media within the jacket, represents a comprehensive six wall cable barrier and furthermore, completely enclosing wiring between physical security perimeters with a second protective measure such as a conduit, would be unduly burdensome, increase the risk of creating adjacency hazards and would not significantly improve the security posture of the critical cyber assets in the electronic security perimeter. Detroit Edison further supports the use of alternative protective measures such as data encryption where technically feasible, over the use of conduit,

Entity	Segment	Vote	Comment
			which significantly provides enhanced security over the use of conduit alone.
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The examples of cable protection cited in the comment appear to be viable physical approaches; however, the conclusion that a six-wall bounded physical solution is the only acceptable one is not accurate. The Requirement R1.1 of CIP-006-1 clearly states that “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 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 or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	5	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that “Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter.			

Entity	Segment	Vote	Comment
The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and 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 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 or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	5	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Manitoba Hydro	5	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			

Entity	Segment	Vote	Comment
Northern States Power Co.	5	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Pacific Gas and Electric Company	5	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” i not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			

Entity	Segment	Vote	Comment
PPL Generation LLC	5	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Reliant Energy Services	5	Negative	Reliant Energy is in agreement with the following comment posted by First Energy at 3:54 pm on August 13, on PJM’ NERC Standard e-Room. That is; “he definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly; the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: On the matter of wiring, it is clear that the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response drafting team agrees that protection can be provided through alternative measures that include use of a combined/complementary physical and logical approach to achieve the same or better protection.			
Salt River Project	5	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			

Entity	Segment	Vote	Comment
Southern California Edison Co.	5	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team' proposed interpretation for CIP-006-1's Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." CE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE's communications network, and the data which streams across it, is strictly controlled by an Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.

Response:

The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.

However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.

The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current

Entity	Segment	Vote	Comment
Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	5	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: • These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. • The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. • The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations. We believe

Entity	Segment	Vote	Comment
			that the Standard Authorization Request should be modified to address concerns and issues related to: • Unauthorized access to the ESP through access to physical cabling. • Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Tennessee Valley Authority	5	Negative	The factors, which lead to this conclusion, are the exponential increase in scope and cost for the implementation of physical security applied to the communication media.
Response: CIP-006-1 requires all Cyber Assets within an ESP to be enclosed within a PSP. The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets "alternative measures" to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden.			
U.S. Bureau of Reclamation	5	Negative	This issue raises a question as to the NERC requirements for the physical protection of critical cyber assets that fall outside of readily defined Physical Security Perimeters (PSPs). The connection between the two PSPs is a communications line employing a routable protocol and may be based on microwave, radio, copper, or fiber technologies. For circuits that go between physical structures separated by more than several feet, the 6 wall requirement is impractical. NERC's response to the question raised was consistent with their overall requirements in the sense that they did not relax protection requirements for Critical Cyber Assets (specifically wiring) external to an Electronic Security Perimeter (ESP). Reclamation will be significantly impacted by this interpretation for its Critical Cyber Systems that extend over several physical sites. Specifically in cases where those sites are interconnected with communications circuits employing "routable protocols." In those instances, since physical protection of the circuits will be impractical or impossible, Reclamation will need to employ "alternate protective measures" on communications lines interconnecting the physically distinct sites. We suggest NERC reconsider their requirements in cases where interconnections between sites remain within the same "control system" and where those interconnections are carried over privately owned circuits. The

Entity	Segment	Vote	Comment
			requirements NERC has outlined make very good sense (and we support them) where the connections go to external entities or where they are carried over public networks. We have no desire to change this aspect of the requirements. We are requesting special consideration be given to private networks between physical and electronic perimeters where those networks are owned/operated by the entities in question.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. The RFI response team is limited to interpreting the requirement of the existing standard. The request for consideration of private networks is best addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project.			
AEP Marketing	6	Negative	Physical protection (given the relatively controlled locations of some of the data paths in question) should be determined by a risk-based assessment. This would be particularly focused on the likelihood of intrusion given the overall physical environment and other factors (cables buried, guard forces, monitoring cameras, etc.), some of which may qualify as acceptable alternative measures. We believe that this topic should be addressed during the formal development of the next iteration of CIP standards to clarify requirements and include risk factors and a rational, realistic approach. For example, securing a facility housing coal handling systems makes complete sense from a potential intrusion perspective. This is less the case with the cabling running externally from the facility to the control room, often buried and not easily or in obtrusively accessible. Because of the factor listed above, AEP is casting a negative vote for this interpretation. We would prefer that it be addressed fully during the development of the next set of NERC CIP standards.
Response: The RFI response drafting team agrees that this is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Consolidated Edison Co. of New York	6	Negative	The interpretation is not clear and may modify the intention of the Standard and needs more work. The existing Standard requirement clearly states, "..all Cyber Assets in an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter", which must be protected.
Response: 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			

Entity	Segment	Vote	Comment
needs to be protected. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
FirstEnergy Solutions	6	Negative	FE thanks the SAR team for their efforts in developing an interpretation for CIP-006-1 Req. R1.1 in response to Progress Energy's request. However, we have cast a Negative vote for the following reasons and ask the team to consider our comments and suggested revision. We feel that the proposed interpretation fails to provide the industry with a clear direction related to the question posed by Progress Energy. As stated, the interpretation largely restates the definition of a Cyber Asset contained in the NERC Glossary of Terms, and a re-statement of CIP-006 R1.1. The interpretation states that "The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network." However, the actual definition from the NERC Glossary states that Cyber Assets include programmable electronic devices and communication networks including hardware, software, and data." Further, in the CIP standards development process the communications paths were deliberately excluded from the scope of the Standards, especially third party communication assets. Accordingly, we concur with the aspect of the interpretation that implies that the communications hardware devices and closets that include critical cyber assets should be secured inside the PSP, but that the physical utility-owned wiring should not be classified as Cyber Asset as the interpretation indicates. This would be consistent with the explicit exclusion of the third party communication assets embodied within the standards. We agree that the definition includes the data as a Cyber Asset, but do not agree that the definition includes the physical wiring as a Cyber Asset. Accordingly as a potential modification to the interpretation, we suggest a revision to the interpretation as follows: "The definition of a Cyber Asset includes the data and the communication network including hardware, software, and data, however, the physical communication wiring that comprises the physical media supporting the network is not a Cyber Asset. The intent of the requirement is to protect the communication data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures."
Response: The RFI response drafting team asserts that physical media (wiring) is a component of a communication network within an ESP and shall be secured inside the Physical Security Perimeter. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and 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 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			

Entity	Segment	Vote	Comment
physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption or monitoring for circuit disruptions due to physical tampering.			
Lincoln Electric System	6	Affirmative	Any wiring within the electronic security perimeter must be protected by a six-wall physical security perimeter. Wiring external to the electronic security perimeter constitutes a "communications link", and therefore does not need to be protected by the physical security perimeter. It appears that some confusion on this issue stems from the fact that Progress Energy's original question isn't even possible - it pertains to wiring within the electronic security perimeter, but outside the physical security perimeter. According to Requirement 1.1, the electronic security perimeter must be a subset of the physical security perimeter. Therefore, any wiring within the electronic security perimeter must also fall within the physical security perimeter by default.
Response: Thank you for your comment. The RFI response drafting team agrees that the configuration in this instance involves two physically separate Cyber Assets that are collectively within a single ESP. Therefore, the interconnecting wiring shall comply with requirement R1.1 of CIP-006.			
Madison Gas and Electric Co.	6	Negative	We disagree with the interpretation because it adds language that needs further interpretation and does not address our confusion in the Standard regarding when data traveling over a network needs to be protected and when it does not. The interpretation implies the measures referenced in CIP006, R1.1, focus on preventing physical access that would allow data to be tampered with in transit. Can we assume the focus is not on preventing physical access that allows data to be gathered/inspected, but rather to prevent tampering with the data? If so, would using optical fibers carrying data communication between two physical security perimeters be a sufficient physical control, assuming fiber provides a higher level of security to protect the data from tampering. Do optical fibers contained within a continuous, fully-jacketed cable, the only end points of which are contained within separate six-sided physical security perimeters, meet the requirements of the Standard under this interpretation? If not, what constitutes the physical security perimeter and what constitutes a physical access point? Please provide guidance, including examples, on the "alternative protective measures" that would be acceptable to meet the standard. The standards are confusing because of the explicit exemption under the Introduction section, Item 4.2.2, of each standard that excludes "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." We assume "communication networks" and "communication links between discrete ESP's" are two different things, since they are referenced separately in other parts of the Standard. Communication links between discrete ESP's are referenced in CIP-005, R1.3, as being outside of the ESP. This reference does not help to clarify the exemption. In addition, communication networks are not referenced in CIP-005, R1.3, or anywhere else except in the definition of Cyber Assets. To say that communication networks are exempt from the Standard implies the data traveling on those networks are also exempt. If this is incorrect, what is NERC's interpretation of the explicit exemption? From a protection standpoint, if there is a difference between the wire and the data traveling across the wire, that needs to be explicitly defined. Where does the Standard state whether data traveling between ESP's does or does not have to be protected?

Entity	Segment	Vote	Comment
Response: The RFI response drafting team agrees that protection of data in motion is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. This request from Progress Energy must be addressed in the formal interpretation process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. 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. The RFI response drafting team disagrees with the commenter that exemption in R4.2.2 applies because the specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside a single ESP. Since the connective wiring is inside the ESP, Requirement R1.1 of CIP-006-1 indeed applies. In the revised response to Progress Energy, the drafting team interprets alternative measures to include approaches that are 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 or monitoring for circuit disruptions due to physical tampering.			
Manitoba Hydro	6	Negative	Manitoba Hydro agrees with the part of the interpretation provided by the SAR drafting team that protection of the data transmitted over wires within an Electronic Security Perimeter as the intent of the requirement. This provides more flexibility to meet the standard by allowing not only physical protection of the wire, but also alternative protective measures for the data such as encryption. Responsible Entities should take reasonable measures to protect the data within an Electronic Security Perimeter. However, Manitoba Hydro does not agree with the part of the interpretation provided by the SAR drafting team that "the definition of a Cyber Asset includes both the data and communication networks, including the wiring that comprises the physical media supporting the network." It should be made clear that the wiring within an Electronic Security Perimeter is considered as part of the Cyber Asset (programmable device or communication network) and that wiring is not itself a Cyber Asset. Since the term communication network is not a NERC defined or clearly understood industry term, the interpretation should not use communication network (or network) as part of any clarifying statement.
Response: The RFI response drafting team agrees and submits a revised interpretation response stating the definition of Cyber Asset in the NERC Glossary includes communication networks. Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. However, the drafting team disagrees with removal of the term communication network in the RFI response, as it already referenced in the NERC Glossary.			
PP&L, Inc.	6	Negative	Response: The definition of a Cyber Asset includes both the data and the routable protocol-based communication network, including the wiring that comprises the physical media supporting the network. The

Entity	Segment	Vote	Comment
			intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures. Alternative protection measures could include 24 x7 monitoring, alerting, and logging of attempts at or actual compromise of the network. Supporting information: Based on CIP-002, R3, the definition introduced by the Interpretation should be limited to the "routable protocol-based" communication networks associated with Cyber Assets.
Response: The RFI response team agrees with the comment that the objective is to protect the data. To do so requires measures to prevent tampering of Cyber Assets. However, the RFI response team disagrees with the last point. The drafting team asserts that the requirement R1.1 does not limit application of alternative measures only to “routable protocol-based communication networks” and therefore doing so is unjustified.			
Salt River Project	6	Negative	In cases where the building hosting the Critical Asset is under control of the Registered Entity, the building itself should serve as the six sided physical container. The possibility of an employee, contractor or guest pulling up a floor panel or ceiling tile, finding the right cable or fiber, and then having a way to tap or monitor the line is not a credible threat
Response: The building hosting the Critical Asset, when under the control of the Responsible Entity, is a qualified Physical Security Perimeter only when access is controlled per CIP-006-1 and all personnel with unescorted access have met the applicable requirements of the CIP standards, including completion of personnel risk assessments and training. If the entire building is not a qualified PSP, then alternative measures must be applied to protect wiring not enclosed within the qualified PSP(s) within the building.			
Southern California Edison Co.	6	Negative	Southern California Edison Company (SCE) SCE appreciates the opportunity to provide comments on the NERC Standards Development team’s proposed interpretation for CIP-006-1’s Requirement 1.1 (Proposed Interpretation). SCE cast a negative vote on the Proposed Interpretation because it causes additional confusion and could result in unreasonable and impractical consequences that would not improve the security of the Cyber Assets or the Electronic Security Perimeter. SCE believes issues identified by Progress Energy should be addressed during the review of CIP-006 scheduled to take place in 2009. Supporting reasons for this position are provided below. The proposed interpretation states that “Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network.” SCE shares a concern raised by WECC in their position paper that if the physical media used to transport critical data is considered a Critical Cyber Asset, then it would require all of the requisite physical protections specified in the existing CIP standards. SCE feels physical media supporting the network cannot be subject to the physical protections specified in CIP standards. For example, if a network cable runs from a Critical Cyber Asset situated within an identified Physical Security Perimeter to a point or through any area that is outside the identified Physical Security Perimeter, it is not clear that taking measures to protect the cable from tampering, and potentially having to monitor access to the cable, would be an appropriate way to secure the network. Access to SCE’s communications network, and the data which streams across it, is strictly controlled by an

Entity	Segment	Vote	Comment
			Electronic Security Perimeter which personnel and equipment/ application(s) are given narrow access rights dependent on their usage requirements. The allowance of "alternative protective measures" for physical media supporting the network is also not clearly defined, and could even be interpreted to allow for logical protections without physical protection of Cyber Assets. This clearly would not be an appropriate outcome as pointed out in WECC's position paper as well. The uncertainty created by the interpretation's reference to alternative protective measures is another reason SCE voted against the interpretation. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances. In closing, it is SCE's opinion that the Proposed Interpretation and the issues brought-up in relation to the actual definition of Cyber Asset be fully addressed and incorporated into the revised CIP-006 standard. Pursuant to NERC's Reliability Standards Development Plan an effort to revise the CIP standards will be initiated in 2009.
Response: The RFI response drafting team acknowledges that the issue of data in motion (among others) is important and is being addressed by the CSO706 Project work that is ongoing. The RFI response drafting team also agrees that Critical Cyber Asset classification is an important issue, and it is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining whether physical protection is required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy. The drafting team recognizes there are instances that pose technical and/or costly challenges to protection of Cyber Assets and clarifies that the current Requirement includes the use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. To the commenter's point regarding more prescriptive and specific language, the drafting team believes that it could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Tampa Electric Co.	6	Negative	Tampa Electric Company's Response to Interpretation of CIP006-1 We would like to thank Progress Energy and the Cyber Security Drafting Team for bringing this concern to the industry's attention and attempting to clarify this issue. Tampa Electric Company has several concerns with the proposed interpretation as currently worded. This interpretation asserts that we must employ physical security (or alternative methods) to protect the wiring. While this type of approach may be achievable in a data center environment where the electronic security perimeter (ESP) is self contained within a room or a single building, it presents an enormous challenge from a generation distributed control system (DCS) perspective where an ESP spans multiple buildings. Additionally, many DCS implementations include remote human machine interfaces which are within the ESP, but distributed throughout the plant. The cost to physically protect the wiring in these environments to the level

Entity	Segment	Vote	Comment
			of CIP006 requirements would easily run into the millions of dollars for a single facility. Running the cable within conduit and encasing in concrete, which is common in many facilities, would still be insufficient to meet the monitoring, logging, and access control requirements of CIP006. In short, physical security solutions to this problem are not practical or cost effective based on the risk being mitigated. Alternative measures to physical security such as encrypted communication links or network segmentation through firewalls to create smaller, separate ESPs are not technically feasible today for most generation DCS networks: ? These technologies are unproven within a DCS environment and require vendor modifications, which will require extensive testing and coordination between the industry and the vendors. ? The primary DCS vendors in our environment have stated to us that they do not offer or support an approved mechanism for firewalling within the DCS network or encrypting data due to the network protocol and impact to the timing of data delivery across the DCS network. The time-sensitive nature of DCS data traffic makes these approaches impractical and introduces risk to reliability and multiple points of failure that are contrary to the intent of these reliability standards. ? The industry will likely introduce support issues by implementing these measures on their own. It is reasonable to expect that this will take much more time to accomplish than is possible within the existing implementation plan. Therefore, Tampa Electric recommends that the drafting team consider addressing this issue in the upcoming revisions to the standards, rather than issuing an interpretation under the existing standards which is unattainable. The revised standards should address specifically protection that is appropriate to cabling and is cost effective based on the risk being mitigated. The drafting team has already identified the need to consider issues surrounding data in motion, and extended LANS over geographically dispersed locations . We believe that the Standard Authorization Request should be modified to address concerns and issues related to: ? Unauthorized access to the ESP through access to physical cabling. ? Disrupting the operation of the critical cyber assets through tampering or destruction of the physical cabling. ? Alternative approaches to physically securing cable through technical means such as firewalls and encryption. This approach allows the industry and DCS vendors time to develop and implement solutions that enhance the overall security without introducing an excessive cost burden or increasing the risk to reliability.
Response: The RFI response drafting team recognizes the variety of challenges that protection of Cyber Assets pose. In the case of DCS equipment within a power plant environment, the technical issues are especially acute. The drafting team interprets “alternative measures” to include physical and logical approaches to protect the Cyber Asset. For the DCS environment, a combination of approaches is possible to achieve an equivalent level of protection without excessive cost burden. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Xcel Energy, Inc.	6	Negative	While Xcel Energy generally supports what we understand to be the intent of the interpretation, we feel it is not clear and could create further ambiguity. An interpretation should be clear and not create further room for interpretation. As explained to us by a member of the Cyber Security Order 706 SAR Drafting Team, the interpretation is designed to address the situation where there are potentially two separate physical security perimeters (PSP) with assets that are part of the same ESP -- such as two separate rooms, a data center and an operations center, that both have critical cyber assets and individual physical security perimeters. You could

Entity	Segment	Vote	Comment
			still have one ESP for the single building -- however, since the wiring connecting the assets in each of these rooms leaves the physical security perimeters, you need to protect the wiring with a physical boundary (conduit), or encrypt the data. We feel strongly that this interpretation, as written, could be implemented and/or enforced inconsistent with what the drafting team intended, and recommend a new draft of the interpretation, including a diagram, be developed. Also, since this interpretation will likely have a substantial impact on entities, an implementation plan should be considered.
Response: The RFI response drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope. The team understands the desire for more specificity and prescription, such as in a diagram, but believes that could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
California Energy Commission	9	Negative	The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: Physical media (wiring) is a component of a communication network within an ESP, but the wiring itself is not a separate Cyber Asset. The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to "wires within a given facility or campus" and therefore doing so is unjustified. The drafting team has clarified what it interprets "alternative measures" to mean in the revised response and believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Commonwealth of Massachusetts Department of Public Utilities	9	Negative	The interpretation should not include speculation as to the intent of the reliability standard.
Response:			

Entity	Segment	Vote	Comment
The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			
Oregon Public Utility Commission	9	Negative	The interpretation should not include speculation as to the intent of the standard. The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus. If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of "alternative protective measures" is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.
Response: The RFI response drafting team does not speculate but rather interprets the standard as permitting "alternative measures" to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering. 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 and would thus not qualify in and of itself as a Critical Cyber Asset. The drafting team believes the phrase "alternative measures" is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			
Electric Reliability Council of Texas, Inc.	10	Negative	This interpretation is an issue that should be handled through the full Standard review process.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is			

Entity	Segment	Vote	Comment
among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Midwest Reliability Organization	10	Negative	MRO Response: CIP-005-1, R1.3 states: "Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s)." Since it is not within the Electronic Security Perimeter, it does NOT need to be within a Physical Security perimeter that is required in CIP-006-1, R1.1. (Glossary) Cyber Assets: "Programmable electronic devices and communication networks including hardware, software, and data." The MRO disagrees that this includes the "wires". The "communication links connecting" are the "wires" and they are excluded per CIP-005, R1.3. We cannot have one standard saying the wires are included and another saying they are not!
Response: Although the drafting team is limited to respond to this request from Progress Energy, to the point about “communication links” cited in CIP-005-1 R1.3, in this instance it does not apply because the wiring is clearly stated by Progress Energy to be within a single ESP.			
SERC Reliability Corporation	10	Negative	The interpretation indicates that the definition of a Cyber Asset includes the wiring that comprises the physical media supporting the [communications] network -- although this is not included in the NERC Glossary definition. The interpretation goes on to state that the intent is to protect the “data” transmitted over the network within the Electronic Security Perimeter rather than to protect “the facilities, systems, and equipment which if destroyed, degraded, compromised or otherwise rendered unavailable, would affect the reliability of the Bulk Electric System as a whole, not risk to a Responsible Entity’s individual asset” as described in Security Guidelines for the Electric Sector: Identifying Critical Assets. The interpretation merely restates the requirement of CIP-006-1, R1.1 to take (either Physical Security Perimeter or alternative) measures to control physical access of Critical Cyber Assets and adds confusion to the standard by introducing concepts contrary to other reference material provided by NERC.
Response: 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. The RFI response drafting team interprets “alternative measures” to include use of a combined/complementary physical and logical approach to achieve the same or better protection. The alternative measures 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 or monitoring for circuit disruptions due to physical tampering.			

Entity	Segment	Vote	Comment
Southwest Power Pool	10	Negative	SPP believes the concerns raised in this interpretation are too important to let lie in an interpretation. Although the interpretation provides additional guidance about the intent of the standard, it is not good practice to keep the requirement as written. A rewrite of R1.1 under a clear scope is a better way for the industry to understand the intent.
Response: The RFI response drafting team agrees that this is an important issue and indeed is presently being addressed as part of the standards revision work of the Cyber Security Order 706 (CSO706) project. A risk-based assessment methodology for determining which assets need protection and the type of protection required is among the frameworks under consideration in the next iteration of CIP standards covered by the CSO706 project. However, interpretation requests are permitted as part of the standards development process. The work of the CSO706 team is not expected to be completed in time to address this RFI from Progress Energy.			
Western Electricity Coordinating Council	10	Negative	“The interpretation would be acceptable if language is added that limits the application of alternative protective measures to wires within a given facility or campus.” “If the physical media used to transport critical data is to be considered a Critical Cyber Asset, then it will require all of the requisite physical protections specified in the existing CIP Standards. The allowance of “alternative protective measures” is not clearly defined, and could be construed to allow for logical protections without physical protection. If the intent is to allow for logical protections, this could allow for other instances where the physical protection for Critical Cyber Assets is not required, and therefore, logical protections will suffice. This could erode the nature and intent of true physical protection over the long-term. If logical protections are to be allowed, the interpretation should state, in no uncertain terms, which types of protections are allowed, and under which specific circumstances.”
Response: The RFI response team asserts that the requirement R1.1 does not limit application of alternative measures only to “wires within a given facility or campus” and therefore doing so is unjustified. The drafting team has clarified what it interprets “alternative measures” to mean in the revised response and believes the phrase “alternative measures” is neutral in its scope and does not prefer physical to logical and vice versa. Nor does it imply the application of one to the exclusion of the other, i.e., a combination of approaches is possible. The drafting team also believes that more prescriptive and specific language could lead to the exclusion of equally effective measures and therefore has elected to avoid such language.			