NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation of CIP-004-1 for Western Electricity Coordinating Council Project 2009-26

The Interpretation of CIP-004-1 for WECC Drafting Team thanks all commenters who submitted comments on the Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (Project 2009-26). These standards were posted for a parallel 45-day public comment period and intial ballot from February 7, 2012 through March 23, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 38 sets of comments, including comments from approximately 99 different people from approximately 59 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

Summary:

The IDT carefully reviewed all comments in response to the posting for parallel formal comment period and ballot that ended March 23, 2012. In the draft interpretation the IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. While the IDT agrees with several commenters that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term in response to WECC's request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to several minority concerns below. The interpretation is being posted for a recirculation ballot.

- One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision. Other commenters suggest that typing on a keyboard is physical access, and that physical access loses any meaning and would no longer be necessary if escorted physical access did not allow physical interaction with the device. In response, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which

someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

- The IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.
- Several commenters provided suggestions or comments that the drafting team was not able to address and stay within the Guidelines for Interpretation Drafting Teams, and the IDT recommends that commenters provide specific comments to address these issues when the Version 5 CIP standards are posted for comment.
- Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.
- Some commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	Chantel Haswell	FPL Group, Inc.	NPCC	5
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Michael R. Lombardi	Northeast Utilities	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
12.	Bruce Metruck	New York Power Authority	NPCC	6
13.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
14.	Robert Pellegrini	The United Illuminating Company	NPCC	1
15.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
16.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
17.	Brian Robinson	Utility Services	NPCC	8
18.	Saurabh Saksena	National Grid	NPCC	1
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5
21.	Tina Teng	Independent Electricity System Operator	NPCC	2
22.	Donald Weaver	New Brunswick System Operator	NPCC	2
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

2.	Group	Emily Pennel	Southwest Power Pool Regional Entity											X

No additional members listed.

3.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Forrest	Krigbaum	WECC	1
2.	Nick	Choi	WECC	1
3.	Mike	Miller	WECC	1
4.	Erika	Doot	WECC	3, 5, 6
5.	Stephen	Larson	WECC	1, 3, 5, 6
6.	Peter	Raschio	WECC	1
7.	Mark	Tucker	WECC	1, 3, 5, 6
8.	Tedd	Snodgrass	WECC	1
9.	Huy	Ngo	WECC	1

4.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	5, 6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Louis Slade		RFC	5, 6									
4. Michael Gildea		MRO	5, 6									
5. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Michael	O'Grady	RFC	1									
6. Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Troy Rhoades	FE	RFC										
2. M.J. Linn	FE	RFC										
3. Dough Hohlbaugh	FE	RFC										
7. Group	Dean Larson	Kansas City Power & Light	X		X		X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Scott Harris	Kansas City Power & Light	SPP	1, 3, 5, 6									
2. Michael Gammon	Kansas City Power & Light	SPP	1, 3, 5, 6									
8. Group	Gregory Campoli	ISO/RTO Standards Review Committee		X								
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Albert DiCaprio	PJM	RFC	2									
2. Mark Thompson	AESO	WECC	2									
3. Gary DeShazo	CAISO	WECC	2									
4. Steven Myers	ERCOT	ERCOT	2									
5. Ben Li	IESO	NPCC	2									
6. Matt Goldberg	ISO-NE	NPCC	2									
7. Bill Phillips	MISO	RFC	2									
8. Donald Weaver	NBSO	NPCC	2									
9. Charles Yeung	SPP	SPP	2									
9. Group	Jason Marshall	ACES Power Marketing Collaborators						X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. James Jones	AEPCO/SWTC	WECC	1, 4, 5									
2. Shari Heino	Brazo Electric Power Cooperative	ERCOT	1									
3. Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
4.	Bob Solomon	Hoosier Energy	RFC 1										
10.	Group	Marie Knox	MISO Standards Collaborators		X						X		
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Jim Cyrulewski	JDRJC Associates, LLC	RFC	8									
11.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Marcela Caballero	IID	WECC	1, 3, 4, 5, 6									
2.	Israel Gonzalez	IID	WECC	1, 3, 4, 5, 6									
3.	Peter Nguyen	IID	WECC	1, 3, 4, 5, 6									
4.	Mauricio Lopez	IID	WECC	1, 3, 4, 5, 6									
12.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
13.	Individual	Shane Eaker	Southern Company	X		X		X	X				
14.	Individual	Kieth Morisette	Tacoma Public Utilities	X		X	X	X	X				
15.	Individual	Keira Kazmerski	Xcel Energy	X		X		X	X				
16.	Individual	Jay Walker	NIPSCO	X		X		X	X				
17.	Individual	Ronnie Hoeinghaus	City of Garland			X							
18.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
19.	Individual	Thad Ness	American Electric Power	X		X		X	X				
20.	Individual	Randi Nyholm	Minnesota Power	X		X		X	X				
21.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
22.	Individual	Brian J Murphy	NextEra Energy Inc.	X		X		X	X				
23.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
24.	Individual	Michael Falvo	Independent Electricity System Operator		X								
25.	Individual	Kim Koster	MidAmerican Energy Company	X		X		X	X				
26.	Individual	Kirit Shah	Ameren	X		X		X	X				
27.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
28.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
29.	Individual	Andrew Ginter	Waterfall Security Solutions								X		
30.	Individual	Thomas Johnson	Salt River Project	X		X		X	X				
31.	Individual	Andrew Gallo	Austin Energy	X		X	X	X	X				
32.	Individual	Patrick Brown	Essential Power, LLC	X				X					
33.	Individual	John Seelke	PSEG (Public Service Enterprise Group)	X		X		X	X				
34.	Individual	Christina Bigelow	Midwest ISO		X								
35.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
36.	Individual	Joe Doetzl	CRSI	X									
37.	Individual	Darryl Curtis	Oncor Electric Delivery Company	X									
38.	Individual	DANA SHOWALTER	E.ON CLIMATE & RENEWABLES					X					

1. **The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on how a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?**

Summary Consideration:

Most commenters agreed with the IDT that the request for interpretation asks for clarity on the meaning of a requirement. There were a few commenters that believe the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

Some commenters suggested that the interpretation may cause difficulty in providing authorized access to vendors or contractors. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement andthe IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The commenters also suggested that the issue should be addressed in conjunction with the CIP Version 5 development. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT, and requests that commenters who suggested that the issue be addressed in Version 5 of the CIP standards provide specific suggestions when those standards are posted for comment.

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
Midwest ISO	The request is asking for clarity on the meaning of	The request seeks clarification of the meaning of "authorized access." As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
	a requirement.	
Response: The IDT agrees that the request for interpretation asks for clarification on the meaning of a requirement.		
Ingleside Cogeneration LP	The request is asking for clarity on the meaning of a requirement.	WECC has requested a clarification of the definition of "authorized access" to determine if vendor personnel who provide supervised temporary support to Responsible Entities, are subject to CIP-004 R2 through R4. This is a subject of great relevance to Ingleside Cogeneration LP as we require all of our vendors to maintain robust cyber security programs, but agree with WECC that a literal reading of CIP-004 may require dedicated agents from each. Critical vendors such as Cisco or GE do not support an operating model like this - and we would argue that their security training and personnel screening procedures are superior. This subject will become especially prevalent when CIP Version 5 takes effect and all Responsible Entities will be required to have a cyber policy that addresses Cyber System Access. We would like to see this complex issue addressed now, before some precedence is set that proves to be uneconomical or unviable.
Response: Thank you for your comment. The IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT. Therefore, the IDT recommends that the commentor provide specific suggestions to the Project 2008-06 SDT when the Version 5 CIP standards are posted for comment.		

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
NextEra Energy Inc.	The request is asking for clarity on the application of a requirement.	Each of the three questions is asking whether a class of individuals (i.e., temporary vendors and supervisors of vendors) is required to comply with CIP-004 R2, R3 and R4. Thus, the questions are requesting specific confirmation whether one is or is out of compliance based on how these classes of individuals are addressed under CIP-004.
Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement.		
Southwest Power Pool Regional Entity	The request is asking for clarity on the application of a requirement.	The clarification requested by WECC specifically states that the WECC RC seeks clarification on the definition of authorized access "as applied to temporary support from vendors."
Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.		
MidAmerican Energy Company	The request is asking for clarity on the application of a requirement.	The request is asking for clarification on the application of the term “authorized access” in order to determine how to comply in the situation of temporary vendor support.
Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT		

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.		
Northeast Power Coordinating Council	The request is asking for clarity on the meaning of a requirement.	
Dominion	The request is asking for clarity on the meaning of a requirement.	
FirstEnergy	The request is asking for clarity on the meaning of a requirement.	
ISO/RTO Standards Review Committee	The request is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Collaborators	The request is asking for clarity on the meaning of a requirement.	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
Imperial Irrigation District (IID)	The request is asking for clarity on the meaning of a requirement.	
NIPSCO	The request is asking for clarity on the meaning of a requirement.	
American Transmission Company, LLC	The request is asking for clarity on the meaning of a requirement.	
American Electric Power	The request is asking for clarity on the meaning of a requirement.	
Minnesota Power	The request is asking for clarity on the meaning of a requirement.	
Duke Energy	The request is asking for clarity	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
	on the meaning of a requirement.	
Ameren	The request is asking for clarity on the meaning of a requirement.	
United Illuminating Company	The request is asking for clarity on the meaning of a requirement.	
Progress Energy	The request is asking for clarity on the meaning of a requirement.	
Waterfall Security Solutions	The request is asking for clarity on the meaning of a requirement.	
Salt River Project	The request is asking for clarity on the meaning of a requirement.	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
Essential Power, LLC	The request is asking for clarity on the meaning of a requirement.	
PSEG (Public Service Enterprise Group)	The request is asking for clarity on the meaning of a requirement.	
Tampa Electric Company	The request is asking for clarity on the meaning of a requirement.	
CRSI	The request is asking for clarity on the meaning of a requirement.	
Oncor Electric Delivery Company	The request is asking for clarity on the meaning of a requirement.	
E.ON CLIMATE & RENEWABLES	The request is asking for clarity	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
	on the meaning of a requirement.	
Bonneville Power Administration	The request is asking for clarity on the application of a requirement.	
Pepco Holdings Inc & Affiliates	The request is asking for clarity on the application of a requirement.	
Kansas City Power & Light	The request is asking for clarity on the application of a requirement.	
MISO Standards Collaborators	The request is asking for clarity on the application of a requirement.	
PacifiCorp	The request is asking for clarity on the application of a requirement.	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
Southern Company	The request is asking for clarity on the application of a requirement.	
Tacoma Public Utilities	The request is asking for clarity on the application of a requirement.	
Xcel Energy	The request is asking for clarity on the application of a requirement.	
City of Garland	The request is asking for clarity on the application of a requirement.	
Independent Electricity System Operator	The request is asking for clarity on the application of a requirement.	
Austin Energy	The request is asking for clarity	

Organization	The Request is Asking for Clarity on the Meaning or Application of the Requirement	Question 1 Comment
	on the application of a requirement.	
Response: Thank you for your comments.		

2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?

Summary Consideration:

Most commenters agree with the IDT that the interpretation does not expand the reach of the requirement, and one commenter expressed rationale that supports the IDT's interpretation by noting that allowing for the concept of supervised electronic access would expand the reach of the requirement.

One commenter believes that the interpretation expands the reach of the requirement because it uses references to standards that are not part of the standard being interpreted. The commenter suggests that such a reference would set an unacceptable precedent. In response to that concern, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors. That commenter also suggests that the interpretation reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is for physical access. However, the IDT notes that the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.

Some commenters do not believe the interpretation allows for emergency access when needed, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.

Commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES.

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
Omaha Public Power District	Negative	1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access.

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
		Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased.
Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors. **-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** **-The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.**		

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
-Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.		
Bonneville Power Administration	The interpretation does not expand the reach of the standard.	BPA believes that if the drafting team allowed for the concept of supervised cyber access, they would be expanding the scope CIP-004.
Response: Thank you for the comment and supporting rationale that reinforces the IDT's interpretation.		
Northeast Power Coordinating Council	The interpretation does not expand the reach of the standard.	
Southwest Power Pool Regional Entity	The interpretation does not expand the reach of the standard.	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
Pepco Holdings Inc & Affiliates	The interpretation does not expand the reach of the standard.	
FirstEnergy	The interpretation does not expand the reach of the standard.	
Kansas City Power & Light	The interpretation does not expand the reach of the standard.	
ISO/RTO Standards Review Committee	The interpretation does not	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
	expand the reach of the standard.	
Imperial Irrigation District (IID)	The interpretation does not expand the reach of the standard.	
PacifiCorp	The interpretation does not expand the reach of the standard.	
Tacoma Public Utilities	The interpretation does not expand the reach of the standard.	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
Xcel Energy	The interpretation does not expand the reach of the standard.	
NIPSCO	The interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation does not	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
	expand the reach of the standard.	
Minnesota Power	The interpretation does not expand the reach of the standard.	
Duke Energy	The interpretation does not expand the reach of the standard.	
Independent Electricity System Operator	The interpretation does not expand the reach of the standard.	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
Waterfall Security Solutions	The interpretation does not expand the reach of the standard.	
Salt River Project	The interpretation does not expand the reach of the standard.	
Austin Energy	The interpretation does not expand the reach of the standard.	
Essential Power, LLC	The interpretation does not	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
	expand the reach of the standard.	
PSEG (Public Service Enterprise Group)	The interpretation does not expand the reach of the standard.	
Tampa Electric Company	The interpretation does not expand the reach of the standard.	
CRSI	The interpretation does not expand the reach of the standard.	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
Oncor Electric Delivery Company	The interpretation does not expand the reach of the standard.	
E.ON CLIMATE & RENEWABLES	The interpretation does not expand the reach of the standard.	
MISO Standards Collaborators	The interpretation expands the reach of the standard.	
Southern Company	The interpretation expands the reach of the	

Organization	Yes or No The Interpretation Expands/Does Not Expand the Reach of the Standard	Question 2 Comment
	standard.	
Ameren	The interpretation expands the reach of the standard.	
United Illuminating Company	The interpretation expands the reach of the standard.	
Progress Energy	The interpretation expands the reach of the standard.	
Response: Thank you for your comments.		

3. Do you agree with this interpretation? If not, please explain specifically what you disagree with.

Summary Consideration:

The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to the concerns raised by commenters below.

One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision, but the IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.

Some commenters noted that training alone will not prevent a vendor from perpetrating malicious activity. In response, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.

Another commenter agreed with the interpretation while noting that the interpretation may confirm a logistical problem in getting vendor support when a vendor will not submit to the entity's background checks and training. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 CIP SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.

A commenter supported the IDT's rationale by noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent harm, and that granting direct cyber access inhibits that ability.

A commenter in agreement with the overall interpretation suggested that the reference to "authorized access" might be made clearer if, rather than referencing R2, R3, and R4, the interpretation specifically stated what those requirements are. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as

requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.

Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.

Commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Some commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

Commenters suggest that the intent of the standard was to allow supervised/escorted cyber access. The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." Additionally, some commenters believe the interpretation does not allow for necessary emergency access, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements.

Commenters suggest that the interpretation defines or puts bounds on the definitions of "authorized access", "cyber access", and "physical access" and that the interpretation equates "authorized access" with being on the list under CIP-004-1, Requirement R4. The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.

Other commenters suggest that typing on a keyboard is physical access, and that physical access loses any meaning and would no longer be necessary if escorted physical access did not allow physical interaction with the device. In response, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

Commenters suggest that if a Responsible Entity can demonstrate that they can supervise remote cyber access, then that access should be allowed. The IDT believes that the relevant question to resolve is not whether an entity can supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized.

Commenters suggest that since "authorized access" is not in the standard, use of the phrase in the interpretation expands the reach of the standard. In response, the IDT notes that it sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.

Some commenters noted concern that the interpretation's reference of other standards sets a bad precedent, but the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.

One commenter agrees with the conclusion of the interpretation, but believes that the request for interpretation is asking for compliance guidance and that the interpretation only restates information in the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

Organization	Yes or No	Question 3 Comment
Alberta Electric System Operator	Abstain	The AESO agrees with the interpretation of CIP-004, however we are casting an abstain vote as this standard is not applicable in Alberta at this time.
Response: Thank you for the comment.		
Consolidated Edison Co. of New York	Affirmative	See NPCC region-wide group comment form

Organization	Yes or No	Question 3 Comment
Response: See NPCC response		
California ISO	Affirmative	Comments form provided jointly with ISO/RTO Standards Review Committee
Response: See ISO/RTO response		
Electric Reliability Council of Texas, Inc.	Affirmative	ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee.
Response: See ISO/RTO response		
Midwest ISO, Inc.	Affirmative	We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access.
Response: "We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision." **The standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.** "The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity." **Whether temporary or permanent, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** "Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access."		

Organization	Yes or No	Question 3 Comment
The IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.		
Cowlitz County PUD	Affirmative	The interpretation is correct. However it does confirm a logistical problem: how to obtain vendor support when the vendor will not submit to the entity's requirement for background checks and training. If the cyber system is broken and can only be fixed via vendor support, the time to get an Exception approved or replace the cyber asset could have a serious negative impact on the BES.
Response: Thank you for the comment. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.		
Wisconsin Energy Corp.	Affirmative	Comments are requested to be submitted using the separate electronic comment form rather than with the vote. While the answer gets a bit circular, and there is room for disagreement in the industry on the interpretation, I support it and do not have any specific comments to submit with this vote.
Response: Thank you for your comment.		
Southwest Power Pool Regional Entity	Yes	The SPP RE agrees with the interpretation, noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent the escorted individual from overtly, covertly, or inadvertently causing harm. Granting direct cyber access to someone without authorized access inhibits the ability to perform

Organization	Yes or No	Question 3 Comment
		the escort responsibilities and introduces risk. As noted in the interpretation, this is why the standard specifically makes a distinction regarding "authorized, unescorted" physical access. Technically, escorted cyber access is not feasible. The SPP RE agrees that "over the shoulder" viewing via a webinar or close proximity presence, while possibly subject to the entity's CIP-003/R5 information protection program, does not constitute cyber access.
Response: Thank you for the comments and rationale, which supports the IDT's interpretation.		
Tacoma Public Utilities	Yes	Agree with the standard as written in the WECC position paper
Response: Thank you for the comment.		
American Electric Power	Yes	AEP agrees with the overall interpretation, but offers the following commentsand recommendations for improving the interpretation.Responses to Questions 1 and 2:The response provided for Q1 does not definitively answer the question that was posed. The question posed asks what the definition is for "authorized access", while the response essentially states that one has this access by being on the proper list. It is not clear from the response how those on the authorized list were added to it, i.e. that those individuals met the necessary training, risk assessment, and access requirements. This might be made clearer if, rather than generally mentioning R2, R3, and R4, specifically stating what those requirements are.The response provided for Question 2 more adequately addresses Question 1 than does the response to Q1.
Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.		
PSEG (Public Service Enterprise Group)	Yes	The inability to provide Escorted Cyber Access through a web-conference (or otherwise), can be detrimental to the reliability of the BES as the time to

Organization	Yes or No	Question 3 Comment
		troubleshoot cyber/networking issues can be extensive without letting the remote support personnel have access to the troubled device.
Response: Thank you for your comment. The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Additionally, given the provisions for emergency access and the ability to plan in advance for authorizing access, the IDT does not believe this interpretation increases the risk level to the BES.		
Tampa Electric Company	Yes	Although we believe that the Interpretations Drafting Team has correctly provided the interpretation, we believe that the standard should be changed to provide a vehicle for emergency vendor access via cyber or physical escorting. The lack of the ability to provide this emergency access could be detrimental to the reliability of the grid and may force Entities into non-compliance to meet the emergency situation.
Response: -Thank you for your comments. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability. Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability. **-The IDT notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.**		
Oncor Electric Delivery Company	Yes	Oncor Electric Delivery agrees with this interpretation. The interpretation provides greater clarity on how a Compliance Enforcement Agency (CEA) addresses "cyber access" which includes both physical and remote acc

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comments		
Dominion	The interpretation expands the reach of the standard.	The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard.
Response: The requirement language addresses “electronic access,” and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of “escorted” supervision for individuals with electronic access, it does not include a provision for “escorted” cyber access. Thus, any electronic access, whether “escorted” or not, must be authorized pursuant to the CIP-004 requirements.		
ACES Power Marketing Collaborators	The interpretation expands the reach of the standard.	Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines “authorized access’ by stating that an individual has “authorized access” if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated “authorized access” with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this

Organization	Yes or No	Question 3 Comment
		reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device.
Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).		
NextEra Energy Inc.	The interpretation expands the reach of the standard.	It could be viewed that the interpretation requested tends to expand the reach of CIP-004, given the lack of clarity in the answers. Thus, if this interpretation goes forward, it is recommended that that the following clearer and more to the point answers be substituted for the current answers, so there is no expanding of CIP-004 nor an elaboration on how the standard applies to particular facts:1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors. Answer: The term authorized access as used in CIP-004 is not limited or qualified by any type or class of employees or vendors. Thus, all employees and vendors (who desire either physical or cyber access) without regard to whether they are temporary support or not must either: (1) be escorted by someone with authorized unescorted physical or authorized cyber access, as applicable or (2) have been granted authorized unescorted physical or authorized cyber access by meeting the requirements of R2 and R3. Thus, there is no exception for temporary support from vendors, and the term authorized access applies to them in the same manner it applies to any other class or type of employee or vendor. 2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?Answer: Yes. The language of CIP-004 applies to all employees and vendors that desire

Organization	Yes or No	Question 3 Comment
		unescorted physical or cyber access to Critical Cyber Assets without regard to whether or not the employee or vendor is supervised. 3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? Answer. See answer to question 2 - supervised vendors are not exempt from CIP-004-1, Requirements R2, R3, and R4, thus the remainder of the question is moot.
Response: The IDT considered these suggestions. The IDT believes that the interpretation adequately addresses that *all* cyber access is contemplated by the interpretation, which includes both employees and vendors. The IDT does not fully agree with the suggested phrase, "be escorted by someone with authorized unescorted physical or authorized cyber access" with respect to CIP-004, versions 2 through 4, and believes that it only exists in version 1 with respect to the 30 and 90 day periods acknowledged in the interpretation's footnote.		
Ingleside Cogeneration LP	The interpretation expands the reach of the standard.	The project team has chosen to differentiate between escorted physical access where a vendor performs a non-cyber activity (such as replacing parts) from one where a cyber connection has been made. Ingleside Cogeneration LP believes the project team has read in extra language into the requirement - and changed FERC's intent in Order 706 paragraph 432. That paragraph was cited by WECC in the original Request for Interpretation, and clearly acknowledges that supervised access is a real-life operational need under certain circumstances. If anything, the Commission brings up a good point about the qualifications of the escort, but it does not seem appropriate that the drafting team has completely ruled out supervised cyber access. Furthermore, by logical inference, if the Responsible Entity can demonstrate that they can supervise remote cyber access, then that should be allowed as well.
Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for		

Organization	Yes or No	Question 3 Comment
individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."		
MidAmerican Energy Company	The interpretation expands the reach of the standard.	WECC is seeking "clarification on the definition of 'authorized access.'"
Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation.		
Midwest ISO	The interpretation expands the reach of the standard.	MISO respectfully submits that, based on a literal reading of the plain language of CIP-004, the phrase "authorized access" is not part of the language of the requirement requested for interpretation. The use of a specific term not utilized in the requirement as well as the assignment of a specific meaning and obligations from the requirement at issue to such a term by the Interpretation Drafting Team ("IDT") in its Interpretation expands the reach of the standard.
Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.		
Pacific Gas and Electric Company	Negative	PG&E disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or on-site cyber access). Registered entities should be allowed to provide vendors, which they have engaged, with temporary digitally escorted access. Prohibiting this capability directly affects the safe and reliable operations of the Bulk

Organization	Yes or No	Question 3 Comment
		Electric System. If this interpretation is approved as worded, a valuable support tool could place utilities in a position where reliability suffers to maintain compliance. Let's take one of the well know router companies for example. This company has one of the highest performing Tier 1 support record of any company. When you call their support you reach their Tier 1 support desk which if allowed to be escorted digitally can address most issues within a reasonable timeframe. If escorted digital access is prohibited entities would have to negotiate dedicated Cisco technicians to support their devices. Not only would this be extremely costly, if possible, most importantly it would not be efficient resulting in delays to address the issue at hand. For remote access, technologies such as WebEx, TightVNC, Timbuk2, etc enable strict remote control solutions, this allows someone to provide logical remote control to a system while fully recording and visually observe (e.g., digitally escort) all actions. At any time, the escort observes anything inappropriate they can shut-off access immediately by a click of a button. In reality, allowing, "digital escorting" is much safer than allowing someone physical access to critical assets as the escort can stop any action with a click of a button whereas with physical access the "escort" has to have the capability to physically stop the individual. For on-site cyber access entities should be able to perform these activities in the same manner that they provide escorting to other visitors, through visual observation. Someone with escorted physical access can do more physical damage to critical assets faster than they can do damage typing on a keyboard with an escort observing them. For example, if the escort observes anything inappropriate being typed they can physically interrupt the individual and keep them from hitting the "enter/execute" command; however, someone can grab a handful of fiber cables going into a patch panel and yank them out before an escort could stop them.
Response: The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability or safety.		

Organization	Yes or No	Question 3 Comment
Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 standards are posted for comment.		
Salt River Project	Negative	The interpretation does not clearly define that escorted electronic access is prohibited.
Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.		
Brazos Electric Power Cooperative, Inc.	Negative	See comments provided by ACES Power Marketing.
Response: See ACES response		
Southwest Transmission Cooperative, Inc.	Negative	Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines "authorized access' by stating that an individual has "authorized access" if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated "authorized access" with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since

Organization	Yes or No	Question 3 Comment
		Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device. This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary

Organization	Yes or No	Question 3 Comment
		to the interpretation, most (probably all) registered entities have a formal process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed. We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert,software expert).
Response: -The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted"		

Organization	Yes or No	Question 3 Comment
cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc). **-The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** **-Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. However, the CIP IDT encourages the commenter to provide specific suggestions to address this issue when the Version 5 CIP standards are posted for comment.**		
Central Lincoln PUD	Negative	The interpretation effectively disallows vendor cyber access, since vendors will be unwilling to undergo training established by each of their customers. The resulting lack of support will add risk to the BES.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.**		
City and County of San Francisco	Negative	While in theory we believe the interpretation makes sense, its real world application is likely to result in undesirable consequences with respect to vendor support of control system maintenance, and have a negative impact on BES reliability. We believe that the concept of requiring a responsible Entity to have document that its vendor has personnel risk assessment program and cyber security training may be

Organization	Yes or No	Question 3 Comment
		worth exploring.
Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.**		
Essential Power, LLC	Negative	Comments: In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation. In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support. Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the

Organization	Yes or No	Question 3 Comment
		reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard. There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.**		
Salt River Project	Negative	As written the interpretation does not clearly define that escorted electronic access is prohibited.
Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.		
U.S. Army Corps of Engineers	Negative	In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1

Organization	Yes or No	Question 3 Comment
		Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, we do not believe the interpretation allows for emergent electronic access when needed. Many companies believe there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, the risk level to the BES, in terms of reliability, is increased.
Response: Response: -While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. **-In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.** **-The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**		
Salt River Project	Negative	The interpretation does not clearly provide a definition that escorted electronic access is prohibited.
Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for		

Organization	Yes or No	Question 3 Comment
individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.		
Dominion	No	The following Dominion responses are provided in order of the questions asked by WECC:1. The interpretation that individuals on the list of personnel authorized for cyber or unescorted physical access to CCAs are subject to CIP-004-1 R2, R3 (with allowed restrictions), and R4 is appropriate.2. CIP-004-1-R4 specifically addresses authorized access and does not state that "all cyber access to Critical Cyber Assets must be authorized". CIP-004-1-R2 and CIP-004-1-R3 (with allowed restrictions) apply to "personnel having authorized cyber or authorized unescorted physical access". The lack of an expression such as "escorted electronic access" does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard.3. The concept of "escorted electronic access" is absent from CIP-004-1. Absent a standard, it should be up to each Registered Entity to determine by internal policy whether or not escorted electronic access should be allowed.
Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.		
Pepco Holdings Inc & Affiliates	No	It is understood why the SDT applied a strict interpretation which results in no change to the existing standard. The requested interpretation would have changed the meaning and reach of the standard. However there still remains a very serious real problem. There is a need to allow cyber access to a vendor on some sort of an emergency basis without meeting R2 and R3. The Impact Statement in the Request for Interpretation submitted by WECC is a very serious problem for many entities that could result in a high risk or serious system reliability problem.
Response: The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk		

Organization	Yes or No	Question 3 Comment
assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.		
FirstEnergy	No	There is an inherent flaw in the interpretation because it is based on an inactive standard CIP-004-1. The current effective standard is CIP-004-3 which differs in a significant way from CIP-004-1. Version 3 of this standard now allows exceptions in emergency situations as stated from the phrase "except in specified circumstances such as an emergency" which is included in R2.1 and R3. This specifically affects the answer to WECC's third question. Remote and on-site cyber access should be allowed under supervision during emergency situations and it would be very difficult to assure that all personnel offering remote assistance in these situations were assessed per the requirements of CIP-004.A second inherent flaw is that the interpretation is based on an inactive standard CIP-006-1. The current effective standard CIP-006-3 expressly describes visitor supervision requirements. Per CIP-006-3, R1.6, visitors are required to be continuously escorted within Physical Security Perimeters. This revised requirement should be integrated into the answers to WECC's second and third question.Therefore, we suggest the team revise the interpretation to only make reference to the current Version 3 standards, and add language in the interpretation that there are exceptions for emergency situations as specified by the entity per CIP-003 which requires details of those emergency situations.
Response: The IDT considered all versions of the CIP standards throughout the Interpretation process as entities could still undergo audit proceedings to CIP Version 1. When an interpretation is requested for an ealier version of a standard, and the issue for which interpretation is requested persists in subsequent versions, the interpretation applies to all of the versions of the standard in which the language being interpreted exists. With regard to the emergency exceptions, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 (which is retained in subsequent approved versions) to allow exceptions to the training and personnel risk assessment authorization requirements in specified		

Organization	Yes or No	Question 3 Comment
circumstances, including emergency situations.		
ACES Power Marketing Collaborators	No	This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus, maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. Three terms are defined or bounded outside the standards development process. These terms include: authorized access, cyber access and physical access. We will not repeat our arguments regarding this expansion of the standard here. They can be found in question 2. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary to the interpretation, most (probably all) registered entities have a formal

Organization	Yes or No	Question 3 Comment
		process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed.We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert, software expert).
Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations, which is consistent with FERC Order No. 706, Paragraph 431. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.		

Organization	Yes or No	Question 3 Comment
-The IDT notes that the FERC Order No. 706 issued directives for development of the CIP standards, and the approved standards that resulted from consideration of Order No. 706 are the relevant requirements that are mandatory and enforceable on Responsible Entities under a particular standard. FERC Order No. 706 itself does not create or allow an exception to a reliability standard. Furthermore, the IDT disagrees that Paragraph 431 merely directs that "limited exceptions should be allowed"; rather, Paragraph 431 suggests that the limited exceptions to required training before obtaining access relate to specific conditions, "such as during emergencies, subject to documentation and mitigation." (FERC Order No. 706, Paragraph 431). That is consistent with the IDT's recognition of the provisions for emergency and planned access. -Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. -With regard to the emergency exceptions and FERC Order No. 706, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 and beyond to allow exceptions to the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. -In response to the comments submitted in regard to an entity's list, maintenance of a list, management approval processes, and list inconsistencies with actual physical and cyber access controls, the IDT cannot make interpretations on how specific entities are achieving compliance. The IDT understands the concerns raised by the commenter, however the IDT understands that each entity has unique processes for achieving and demonstrating compliance.		
Southern Company	No	Comments: Question 2 and 3 from the Request for Interpretation are not answered by the interpretation. The answers simply describe how the CIP standards do not address the questions being asked. The standards do not address the scenario contemplated by the line of questioning and should be remanded to the CIP SDT to fix in version 5 of the standards.Comment:Vendor support personnel dispatched to the various generation sites are selected base upon their physical availability and the expertise required on the projects. It is a difficult task to provide ongoing training and background checks for every potential individual from numerous vendors supporting a variety of systems. It is near impossible to monitor the ongoing employment status of this large number of vendor personnel, to assure timely removal from the access control list, that will be required if implemented as discussed in the proposed interpretation.At present, vendor personnel supplying

Organization	Yes or No	Question 3 Comment
		setup/support may work freely on pre-shipped non-installed systems. This trusted relationship should be extended, to similar individuals under escort at the equipment site. If the support function requires that changes be made to systems, having site personnel follow the direction of the vendor expert presents an increase potential for error, while adding marginal security benefits.
Response: Thank You for your comment. The IDT must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. Modifications to an approved Standard must be addressed within the Standards development process, the IDT encourages the commenter to submit the comments to the SDT working on CIP V5.		
City of Garland	No	Disagree with the concept of there being no escorted Cyber Access. If someone with authorized access is working with a vendor or contractor on an issue, the system is more secure than if you give him authorized access just because he has a PRA and has had CIP training. Take for example, Hector Xavier Monsegur, the notorious hacker known as Sabu and leader of LulzSec. Because of his cooperation and work with the FBI and other agencies, he may end up with his record cleansed or at least be able to put on a resume his work with the FBI. Eight years from now, a 7 year criminal background check could be clear. If a company were to utilize him for a short term issue, would the company be more secure with him being "escorted" or with him being issued authorized access and allowed free access. It is noted in your supporting comments that the standard requirements do not state specifically that escorted cyber access is permitted. On the other hand, the standard requirements do not have statements preventing escorted cyber access either. Which is more secure?
Response: -Thank You for your comment. While the effectiveness of personnel risk assessment and Training controls are an interesting theoretical discussion, the IDT must provide an interpretation that meets the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.		

Organization	Yes or No	Question 3 Comment
-While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.		
NextEra Energy Inc.	No	As written, this interpretation should either be dismissed as in appropriate or the answers re-written to be clearer and more responsive. See answers to question 1 and 2.
Response: Thank you for your comment. See response to commenter in Question 2.		
Ingleside Cogeneration LP	No	Ingleside Cogeneration LP believes that the interpretation is an overly-literal reading of CIP-004 and may hamper routine technical support processes with no demonstrable reduction in cyber-risk . The power and convenience of remote vendor maintenance may be unavailable to all but the largest utilities should costs rise because of it. Such a result will actually diminish BES reliability as access to highly competent technical support and maintenance personnel becomes restricted.There may be acceptable solutions, however. It would seem that a single cyber certification of vendors such as Cisco and GE could be referenced in thousands of individual security policies. Alternatively, the industry could provide a single generic cyber training package and employee background check method for vendors. We would hope that NERC takes a leadership position in resolving these complex issues.Lastly, the industry needs more direction than that provided in the circular response to the first question. The project team essentially states that the Responsible Entity must determine who has authorized access to their Critical Cyber Assets and include them on an access list. That list will then define authorized access - leaving the door open for a wide variety of resolutions.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.		

Organization	Yes or No	Question 3 Comment
-The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." -The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.		
MidAmerican Energy Company	No	The request is asking how to comply with one or more requirements in a specific situation with vendor support. Requests as to how to comply, per the Rules of Procedure, do not meet the valid criteria of an interpretation request. While we agree with the conclusion in the proposed response, the draft response restates information that already is in the standard.
Response: The WECC RFI is seeking interpretation of a requirement, and the IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.		
Ameren	No	The CIP-004 R4 IDT interpretation relies on incorrect logic in stating that Standard does not allow for escorted (supervised) cyber access to cyber assets solely because "unescorted cyber" is not explicitly included in the CIP-004 R4 "list". We agree with the idea put forth in the Requirement that anyone with unfettered cyber access is a potential danger and in like manner, so would anyone with unescorted physical access. However, the reason the Requirement does not require those with escorted cyber access to be listed is not because such access is somehow not contemplated or not permitted but rather because, like escorted physical access, these individuals, and their actions, are well monitored and controlled and do not need the extra care and handling that ensues from being on "The List" for those free to take independent action. The mere fact that they do not need further "handling" does not mean in any way that they do not exist or that this in not permitted. We are concerned that IDT is

Organization	Yes or No	Question 3 Comment
		using a classic argument from the negative to imply something is impermissible on that such use is not contemplated merely because it is absent from a list of threat types that need to be addressed.
Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."		
United Illuminating Company	No	The Interpretation DT correctly states that CIP-004 R2 and R3 apply to individuals on a list designating them with authorized cyber access or authorized unescorted physical access to Critical Cyber Assets. The Interpretation DT makes an error in stating that CIP-004 limits the type of cyber access to a Critical Cyber Assets to only authorized individuals, that is, there is no opportunity to implement supervised remote access via terminal session (i.e. Webex) to support personnel not on the authorized cyber access list.The Reliability standards do not provide a definitive statement of the types of access allowed to Critical Cyber Assets. The Standards only provide the program requirements for three types of access; authorized physical, escorted physical, and authorized cyber. By not providing a definitive list of the types of access the original Drafting team did not exclude the type of access under review in this interpretation, that is, supervised cyber access via terminal session.At the time the Reliability standards was approved the concept of supervised remote access was known. The Interpretation Drafting Team can only conclude that the original Standard Drafting Team did not list specific requirements for this type of access. The Interpretation Drafting Team cannot conclude that this type of access was prohibited. The fact that CIP-007 does not contain a specific unescorted cyber access provision is irrelevant. CIP-007 R5 requires technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Supervised access via Webex is not unauthorized system access. When terminal session access is utilized, the

Organization	Yes or No	Question 3 Comment
		activity is tracked by the Company. R5 does not state all authorized user activity, the Interpretation drafting team is adding the word authorized in its response and is expanding the scope.This conclusion is more sensible for service vendors and SCADA system providers. The Interpretation Drafting Team's interpretation would require, as the requestor noted, large vendors (such as CISCO) to take every entities cyber training course and submit to multiple background checks. This would be compliance for compliance sake and not for security. The Interpretation should have stated that the names of authorized individuals are maintained on a list. These individuals are required to comply with CIP-004 R2 through R4. Supervisory Cyber Access via terminal session is not prohibited explicitly by the Standards and is therefore allowed. There are no additional Reliability requirements for such access beyond those described in Standards CIP-002 through CIP-009.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. -Considering the Standards Development Process is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."		
Progress Energy	No	Progress Energy disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or onsite cyber access). Registered Entities should be able to allow vendors providing support temporary, indirect, and monitored access to in scope NERC CIP assets via remote terminal sessions (Live Mtg, Webex, etc) (just as escorted physical access is allowed) without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. In addition, Registered Entities should be able to allow vendors providing onsite temporary support escorted cyber access without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4.There are multiple NERC CIP support vendors that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard. This

Organization	Yes or No	Question 3 Comment
		includes process control vendors not just IT vendors. Honeywell, GE, ABB, Siemens, Babcock and Wilcox, Emerson, GTE, Wood Group are all DCS vendors/tuners that may need to provide escorted cyber access at Progress Energy and throughout the industry. Not allowing for escorted cyber access could have adverse impacts to BES Reliability since some of this work is needed not only during emergencies but also for ongoing maintenance. Long term service agreements are in place with these vendors that have warranty implications that require escorted cyber support for various process control systems. Many Registered Entities rely on these vendors/tuners to provide their expertise in support of continual operations for proprietary systems and do not employ resources with these specialized skill sets.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** **-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.**		
Waterfall Security Solutions	No?	Unidirectional remote screen view products using hardware-enforced unidirectional communications or "data diodes" can securely show remote, unauthorized personnel the contents of screens on Critical Cyber Assets which are inside of an ESP. The technology allows remote personnel to watch and advise as authorized individuals carry out cyber access to those CCAs without introducing any risk that the remote personnel can directly influence the monitored CCAs in any way. This mechanism addresses WECC's concern regarding being "excessively burdened by limiting access to timely support." Since unidirectional remote screen view technology prevents the

Organization	Yes or No	Question 3 Comment
		unauthorized observer from carrying out any direct cyber access, the unidirectional technology should have been identified in the interpretation as a legitimate form of supervised remote access.
Response: Without commenting on specific technology, this comment raises access control and information protection considerations that are both outside the scope of this interpretation.		
Salt River Project	No	As written we disagree with the IDT team's interpretation of CIP-004. We recognize CIP-004 does not include the concept of any words relating to "escorting" or "supervision" in the requirement language. However, the interpretation is not clearly defined and reaches the conclusion that escorted electronic access is prohibited because a formal electronic access escorting requirement is not defined. It appears this conclusion was based on the fact that CIP-006 clearly defines "escorted" or "supervised" physical access to cyber assets. We believe this type of assumption sets a bad precedent for future interpretations.Additionally we believe this interpretation won't allow emergent electronic access when needed. We believe there is little or no risk associated with allowing escorted access to a known contracted support vendor, when support is needed. In fact we believe prohibiting this type of access increases the risk level to the BES.
Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.**		
Austin Energy	No	We believe NERC should acknowledge that "escorted" cyber access is legitimate. If one of our employees is monitoring the cyber activities of the escorted vendor, our

Organization	Yes or No	Question 3 Comment
		employee could terminate the session if the vendor began to take inappropriate actions. This is akin to the situation for escorted physical access. As long as the person is escorted, if s/he begins to take inappropriate action, the escort can take appropriate responsive action.
Response: As written the Standards do not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.		
Essential Power, LLC	No	In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation.In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support.Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard.There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their

Organization	Yes or No	Question 3 Comment
		functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access.
Response: The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. **Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.**		
Midwest ISO	No	MISO respectfully submits that the IDT's proposed Interpretation of the phrase "authorized access" is unsupported by the plain language of CIP-004. The phrase "authorized access," which is the subject of the Interpretation, does not appear in CIP-004. Instead, the Standard uses the phrase "authorized cyber or authorized unescorted physical access." MISO understands that the question posed by the requestor utilized the term "Authorized Access", but respectfully submits that the IDT should have provided clarification specifically regarding authorized cyber access and authorized unescorted cyber access, which clarification would have resulted in entities ability to more directly apply the interpretation to its compliance efforts under CIP-004-1, R2. Moreover, the IDT's explanation of "authorized access" merely refers back to the requirements associated with access without providing the requested clarification. As a result, MISO does not agree with the Interpretation as to the answer provided in response to Question 1. As to the proposed answers to Questions 2 and 3, MISO respectfully submits that, without the specific clarification requested under Question 1, the Interpretation's conclusions are not sufficiently supported by the text of CIP-004.

Organization	Yes or No	Question 3 Comment
Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.		
CRSI	No	The response to question 1 attempts to define authorized access. The definition, even if local to CIP-004, should be expanded to include an indication that authorized access indicates personnel with approval to access Critical Cyber Assets. The presence of a person's name on a maintained list could be in error and would not be an indication of authorized access.
Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized.		
MISO Standards Collaborators		We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access.
Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard.		
Omaha Public Power District		From NERC Comment form (Sorry we did not get it submitted on time) 1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the

Organization	Yes or No	Question 3 Comment
		application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased.

Organization	Yes or No	Question 3 Comment
Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors. -The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES. -Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.		
Bonneville Power Administration	Yes	
Kansas City Power & Light	Yes	
ISO/RTO Standards Review Committee	Yes	
Imperial Irrigation District (IID)	Yes	
PacifiCorp	Yes	
Xcel Energy	Yes	
NIPSCO	Yes	

Organization	Yes or No	Question 3 Comment
American Transmission Company, LLC	Yes	
Minnesota Power	Yes	
Duke Energy	Yes	
Independent Electricity System Operator	Yes	
E.ON CLIMATE & RENEWABLES	Yes	
Northeast Power Coordinating Council	Yes	
Great River Energy	Negative	Please see the formal comments submitted by ACES Power Marketing.
Brazos Electric Power Cooperative, Inc.	Negative	Please see comments to be submitted by ACES Power Marketing.
FirstEnergy Solutions	Negative	Please see FirstEnergy's comments submitted through the formal comment period.
Occidental Chemical	Negative	See comments submitted from Ingelside Cogeneration LP
Omaha Public Power District	Negative	Please Doug Peterchuck's comments.
Response: Thank you for your comments.		

END OF REPORT