NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation of CIP-004-1 by WECC (Project 2009-26)

The Interpretation of CIP-004-2 Drafting Team thanks all commenters who submitted comments on the interpretation of CIP-004-1 – Cyber Security – Personnel & Training, Requirement R2, R3, and R4, for WECC. This interpretation was posted for a 10-day initial ballot from January 6, 2010 – January 19, 2010. Stakeholders were asked to provide feedback on the interpretation and associated documents through an electronic comment system. There were 80 sets of comments, including comments from approximately 80 different people from approximately 53 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

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.

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

Voter	Entity	Segment
Rick Spyker	AltaLink Management Ltd.	1
Kirit S. Shah	Ameren Services	1
Jason Shaver	American Transmission Company, LLC	1
Donald S. Watkins	Bonneville Power Administration	1
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1
Paul Rocha	CenterPoint Energy	1
Robert Martinko	FirstEnergy Energy Delivery	1
Harold Taylor, II	Georgia Transmission Corporation	1
Ronald D. Schellberg	Idaho Power Company	1
Larry E Watt	Lakeland Electric	1
Terry Harbour	MidAmerican Energy Co.	1
John Canavan	NorthWestern Energy	1
Richard J. Kafka	Potomac Electric Power Co.	1
Kenneth D. Brown	Public Service Electric and Gas Co.	1
Tim Kelley	Sacramento Municipal Utility District	1
Robert Kondziolka	Salt River Project	1
Pawel Krupa	Seattle City Light	1
Richard Salgo	Sierra Pacific Power Co.	1
Dana Cabbell	Southern California Edison Co.	1
Horace Stephen Williamson	Southern Company Services, Inc.	1
Keith V. Carman	Tri-State G & T Association Inc.	1
John Tolo	Tucson Electric Power Co.	1

Chuck B Manning	Electric Reliability Council of Texas, Inc.	2
Kim Warren	Independent Electricity System Operator	2
Kathleen Goodman	ISO New England, Inc.	2
Jason L Marshall	Midwest ISO, Inc.	2
Alden Briggs	New Brunswick System Operator	2
Gregory Campoli	New York Independent System Operator	2
Bobby Kerley	Alabama Power Company	3
Thomas R. Glock	Arizona Public Service Co.	3
Rebecca Berdahl	Bonneville Power Administration	3
Linda R. Jacobson	City of Farmington	3
Russell A Noble	Cowlitz County PUD	3
Jalal (John) Babik	Dominion Resources, Inc.	3
Joanne Kathleen Borrell	FirstEnergy Solutions	3
Leslie Sibert	Georgia Power Company	3
R Scott S. Barfield-McGinnis	Georgia System Operations Corporation	3
Gwen S Frazier	Gulf Power Company	3
Don Horsley	Mississippi Power	3
Terry L Baker	Platte River Power Authority	3
Jeffrey Mueller	Public Service Electric and Gas Co.	3
Kenneth R. Johnson	Public Utility District No. 1 of Chelan County	3
Greg Lange	Public Utility District No. 2 of Grant County	3
James Leigh-Kendall	Sacramento Municipal Utility District	3
John T. Underhill	Salt River Project	3
Dana Wheelock	Seattle City Light	3
Ronald L Donahey	Tampa Electric Co.	3
James R. Keller	Wisconsin Electric Power Marketing	3
Gregory J Le Grave	Wisconsin Public Service Corp.	3
David Frank Ronk	Consumers Energy	4
Guy Andrews	Georgia System Operations Corporation	4
Douglas Hohlbaugh	Ohio Edison Company	4
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4

Mike Ramirez	Sacramento Municipal Utility District	4
Hao Li	Seattle City Light	4
Anthony Jankowski	Wisconsin Energy Corp.	4
Francis J. Halpin	Bonneville Power Administration	5
Alan Gale	City of Tallahassee	5
James B Lewis	Consumers Energy	5
Mike Garton	Dominion Resources, Inc.	5
Kenneth Dresner	FirstEnergy Solutions	5
Gary L Tingley	Portland General Electric Co.	5
David Murray	PSEG Power LLC	5
Thomas J. Bradish	RRI Energy	5
Bethany Wright	Sacramento Municipal Utility District	5
Glen Reeves	Salt River Project	5
Michael J. Haynes	Seattle City Light	5
Martin Bauer	U.S. Bureau of Reclamation	5
Linda Horn	Wisconsin Electric Power Co.	5
Edward P. Cox	AEP Marketing	6
Brenda S. Anderson	Bonneville Power Administration	6
Louis S Slade	Dominion Resources, Inc.	6
Mark S Travaglianti	FirstEnergy Solutions	6
Paul Shipps	Lakeland Electric	6
James D. Hebson	PSEG Energy Resources & Trade LLC	6
Dennis Sismaet	Seattle City Light	6
William Mitchell Chamberlain	California Energy Commission	9
Jerome Murray	Oregon Public Utility Commission	9
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10
Louise McCarren	Western Electricity Coordinating Council	10

Consideration of Comments on Initial Ballot — Interpretation of CIP-004-1 by WECC (Project 2009-26)

Summary Consideration:
Since the previously-posted interpretation, the Interpretation Drafting Team ("IDT") has considered all of the submitted comments, and revised the interpretation. In addition to revisions made to address issues identified by commenters, the team revised the interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. Consistent with the guidance in the Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

Many commenters disagreed with the previously-posted interpretation's statement that there is no effective way to provide escorted or supervised cyber access, and they further noted that it is possible to provide escorted cyber access. Other comments note that escorted or supervised cyber access should be allowed.

The IDT recognizes there may be tools that allow escorted cyber access. However, pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT must consider the words of the standard as written. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, the standard requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.

Additionally, the IDT does not believe the standard allows for escorted or supervised cyber access to cyber assets, but agrees that the standard does allow for escorted or supervised physical access to cyber assets, as explained in the revised interpretation language.

Some commenters expressed concern about limitations in emergency situations. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.

Other commenters noted concern about the reference in the previously-posted interpretation to the FAQ document. The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an

approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access. Although WECC's Request for Interpretation was submitted on CIP-004-1, this interpretation is applicable to all subsequent versions of the standard in which the requirement language for which the interpretation was requested persists. The FAQ was written for Version 1 of the CIP standards and the language concerning authorized access has not been modified to conform to the changes made in subsequent versions.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Shrayshuen, at 404-446-2563 or at herb.shrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[2]

Voter	Entity	Segment	Vote	Comment
Chuck B Manning	Electric Reliability Council of Texas, Inc.	2	Negative	"ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". The remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize the capabilities of whoever is available for support at that time. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement."
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language . As written, CIP-004 requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				

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

Voter	Entity	Segment	Vote	Comment
David Murray	PSEG Power LLC	5	Affirmative	"PSEG agrees that background checks and training are appropriate those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed."
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Gary L Tingley	Portland General Electric Co.	5	Negative	1. NERC needs to better define "authorized access". 2. Authorized access should not include temporary vendor support that is accomplished under the supervision of an authorized individual.
Response: Thank you for the comment. The interpretation language has been revised. The IDT also notes that any change to the standard or associated definitions, such as your comment concerning better defining "authorized access," is outside the scope of the interpretation process. Nonetheless, while the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.				
Edward P. Cox	AEP Marketing	6	Negative	AEP agrees with the SDT's response to question #2 and believes that a similar response should have been provided to question #1 as well. Simply stated, as the SDT described in its first sentence, " . . . the ACE referenced in BAL-002-0 Requirement 4 is ACE as defined in BAL-001-0.1a Requirement 1 . . . " The requesting entity is seeking to have the SDT approve that their particular application of an "adjusted ACE" for the standard is compliant. AEP believes that the definition of ACE, as defined in BAL-001-0.1a R1, provides for adjustments by the ADI as a pseudo-tie falling in the Net Interchange value and by time correction falling in the Frequency Schedule value. In response to the interpretation request, the SDT introduced an equivalent "reporting ACE" term that is not contained within the referenced standard requirements. The SDT then explains the

Voter	Entity	Segment	Vote	Comment
				use of an ACE Diversity Interchange (ADI) in the context of a Reserve Sharing Group (RSG). The use of a new term and the subsequent ADI/RSG discussion modifies the standard requirements by interpretation, which is not consistent with the use of a request for interpretation.
Response: The IDT believes that this comment was intended for a different interpretation's posting and is outside the scope of this interpretation.				
Jason Shaver	American Transmission Company, LLC	1	Negative	ATC appreciates the work of the standards drafting team but disagrees with the proposed interpretation. It is our understanding that the requirements in question apply strictly to those individuals that are granted un-supervised access to a cyber asset or un-escorted physical access of a Critical Cyber Asset. We believe that there are acceptable protocols/ processes that can provide effective supervision of a person within a cyber asset and therefore disagree with the SDT opinion that ""...there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors...". If an entity has protocols/processes in regards to supervision of a person accessing a cyber asset electronically then CIP-004-1 Requirements 2, 3 and 4 would not be applicable to the person being supervised. ATC recommends the following interpretation: CIP-004-1 Requirement 2, 3 and 4 govern the actions of an entity in their dealings over persons with authorized cyber access or authorized unescorted physical access to Critical Cyber Asset(s). In so much that they grant a person un-supervised or un-escorted access to either portions of or all Critical Cyber Assets. These requirements do not apply to persons who are supervised / escorted while they are accessing a cyber asset electronically or physically.
Response: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the				

Voter	Entity	Segment	Vote	Comment
concept or any words relating to “escorting” or “supervision” in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Brenda S. Anderson	Bonneville Power Administration	6	Negative	BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Donald S. Watkins	Bonneville Power Administration	1	Negative	BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Francis J. Halpin	Bonneville Power Administration	5	Negative	BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Rebecca Berdahl	Bonneville Power Administration	3	Negative	BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendor support.

Voter	Entity	Segment	Vote	Comment
The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004.				
Bethany Wright	Sacramento Municipal Utility District	5	Negative	Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used.
Response: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
James Leigh-Kendall	Sacramento Municipal Utility District	3	Negative	Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used.

Voter	Entity	Segment	Vote	Comment
Mike Ramirez	Sacramento Municipal Utility District	4	Negative	Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used.
Tim Kelley	Sacramento Municipal Utility District	1	Negative	Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that this interpretation does not affect an entity's ability to fully vet a vendor pursuant to Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.				
Terry Harbour	MidAmerican Energy Co.	1	Negative	Contrary to the interpretation, MidAmercian believes you can provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that

Voter	Entity	Segment	Vote	Comment
				electronic access
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10	Negative	ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". Remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize their capabilities. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Linda R. Jacobson	City of Farmington	3	Negative	FEUS thanks the drafting team for the interpretation, however, does not fully agree. FEUS SME's decided to vote No on this interpretation. The interpretation does not clarify "authorized access" as it applies to temporary support from vendors for cyber access. FEUS does not agree effective escorted or supervised cyber access cannot be accomplished in some circumstances; such as, an authorized individual working directly with temporary vendor support.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must				

Voter	Entity	Segment	Vote	Comment
comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.				
Douglas Hohlbaugh	Ohio Edison Company	4	Negative	FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support.
Joanne Kathleen Borrell	FirstEnergy Solutions	3	Negative	FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote

Voter	Entity	Segment	Vote	Comment
				support.
Kenneth Dresner	FirstEnergy Solutions	5	Negative	FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support.

Voter	Entity	Segment	Vote	Comment
Mark S Travaglianti	FirstEnergy Solutions	6	Negative	FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support.
Robert Martinko	FirstEnergy Energy Delivery	1	Negative	FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support.
Response: Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments, the interpretation				

Voter	Entity	Segment	Vote	Comment
language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Alan Gale	City of Tallahassee	5	Negative	I am voting no because the standard, as written, allows a 30 day or 90 day grace period to perform the PRA and Training. This provision is removed from Version 2, both have to be performed prior to granting access. An entity could allow access to CCA's and not have the PRA/training done and be compliant if the access is for less than 30-days. While I agree it is not desired, it is allowed as written. The next version does NOT allow it. The Interpretation process cannot be used to start "enforcing" the next version prior to its authorization and implementation dates.
Response: Thank you for your comment. While the original request for interpretation was of CIP-004-1, as you have noted, the 30- and 90-day periods were eliminated in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. The drafting team agrees that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ.				
John Tolo	Tucson Electric Power Co.	1	Negative	I respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, I disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. I believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard,

Voter	Entity	Segment	Vote	Comment
				does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. I am therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." I believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. I believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the IDT disagrees that "authorized access" does not apply to vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	In one part of the response it says "there is no way to provide effective escorted or supervised cyber access" without a PRA and training to ensure that actions of the vendor do not harm. However, even with a PRA and training you still cannot ensure this. This interpretation needs more work.
Response: Thank you for your comment. The IDT has revised the interpretation in response to comments and pursuant to the NERC Guidelines for				

Voter	Entity	Segment	Vote	Comment
Interpretation Drafting Teams.				
Richard J. Kafka	Potomac Electric Power Co.	1	Affirmative	Issue is "escorted access" for cyber assets. Interpretation says that there can be escorted physical access, but there is no such thing as escorted cyber access. Everyone with cyber access, including vendors, must meet the training a background checks for the registered entity's cyber security policy. As difficult as this may be for vendors and their customers, that is no reason other than emergencies to grant an exception to those who may have cyber access.
Response: Thank you for your comment. The IDT agrees, as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Richard Salgo	Sierra Pacific Power Co.	1	Negative	It does not appear that the Drafting Team added any clarity to the term "authorized access" with this interpretation. It is our belief that "authorized access" refers to the authorization of permanent, direct, and unsupervised access to critical cyber assets, and disagree with the assertion that there is no means to provide effective supervision of vendor access to CCA's. We are troubled by the apparent dismissal of guidance provided in the FAQ's, as these FAQ's are heavily relied upon by the industry to guide compliance activities and decisions.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access. The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the				

Voter	Entity	Segment	Vote	Comment
changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation.				
Jalal (John) Babik	Dominion Resources, Inc.	3	Negative	Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability.
Louis S Slade	Dominion Resources, Inc.	6	Negative	Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability.
Mike Garton	Dominion Resources, Inc.	5	Negative	Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability.
Response: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude support vendors.				
Alden Briggs	New Brunswick System Operator	2	Negative	NBSO is voting 'no' due to the physical access issue. Pertaining to physical access, NBSO believes that a person who is escorted by someone that has authorized access (PRA and cyber training) does not need the training. Pertaining to electronic access, NBSO believes all personal that have electronic access need to be trained.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comment. The IDT agrees as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
James D. Hebson	PSEG Energy Resources & Trade LLC	6	Affirmative	PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non-emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed.
Jeffrey Mueller	Public Service Electric and Gas Co.	3	Affirmative	PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed.
Kenneth D. Brown	Public Service Electric and Gas Co.	1	Affirmative	PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed.
Response: Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments and pursuant the NERC's Guidelines for Interpretation Drafting Teams, the interpretation language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an				

Voter	Entity	Segment	Vote	Comment
entity's emergency response procedures.				
Russell A Noble	Cowlitz County PUD	3	Negative	Requirement for vendors to submit to each entity's Risk Assessment and Cyber Training program appears not workable. Once an entity finds a vendor not cooperative, what then? When buying new equipment, vendors are more cooperative. But for older equipment/software there is not much incentive to induce vendors to comply. This forces the entity in a very hard position.
Response: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors.				
Dana Wheelock	Seattle City Light	3	Negative	Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may

Voter	Entity	Segment	Vote	Comment
				cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Dennis Sismaet	Seattle City Light	6	Negative	Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-

Voter	Entity	Segment	Vote	Comment
				1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. Thank you.
Hao Li	Seattle City Light	4	Negative	Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential

Voter	Entity	Segment	Vote	Comment
				confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Michael J. Haynes	Seattle City Light	5	Negative	Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards.

Voter	Entity	Segment	Vote	Comment
				We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Pawel Krupa	Seattle City Light	1	Negative	Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular

Voter	Entity	Segment	Vote	Comment
				guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				
Paul Shipps	Lakeland Electric	6	Negative	Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.				
Larry E Watt	Lakeland Electric	1	Negative	supervised cyber access is possible and manageable by any able cyber security team and should not require the time and expense of training vendors for single access sessions.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is				

Voter	Entity	Segment	Vote	Comment
absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.				
Ronald L Donahey	Tampa Electric Co.	3	Negative	Tampa Electric thanks the Standards Drafting Team for the opportunity to comment during the Initial Ballot for the interpretation of Project 2009-26. , WECC Interpretation. We believe cyber escorting of personnel without specifically authorized access should be allowed without requiring a pre-screening via the Personnel Risk Assessment and pre-NERC training as in a network operation center support arrangement. The support vendors cannot always guarantee the availability of specific support personnel during an emergency or unplanned situation. This leaves a utility in position of potential violation versus a potential reliability issue if this is not resolved. Tampa Electric proposes that NERC establish some type of vendor certification program for the sector that would allow major systems vendors (such as Areva, GE, Emerson,Cisco, etc.) to certify at the energy sector level that they meet the Personnel Risk Assessment and training requirements so that each utility does not need to perform this for personnel who are working throughout the industry for multiple entities. It the interpretation of the drafting team as currently worded is adopted, then we suggest that the certification program be developed first so that vendors can certify to NERC that they meet the requirements which would allow them to be certified for utility purposes. It is our position that the Standards Drafting Team has not sufficiently addressed the question raised by WECC on the supervision or escorted cyber access. Based on these factors, Tampa Electric votes no to the adoption of this interpretation.
Response: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.				

Voter	Entity	Segment	Vote	Comment
James B Lewis	Consumers Energy	5	Negative	The interpretation seems to make the determination that there is “no way to provide effective escorted or supervised cyber access”. Thus, anyone granted any type of cyber access to a critical cyber asset must be compliant with CIP-004 R2, R3 and R4. Our Subject Matter Experts believe that there are acceptable protocols that can provide effective supervision of a person accessing critical cyber assets.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Bobby Kerley	Alabama Power Company	3	Negative	The interpretation states “For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an

Voter	Entity	Segment	Vote	Comment
				employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document.
Don Horsley	Mississippi Power	3	Negative	The interpretation states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. " We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and

Voter	Entity	Segment	Vote	Comment
				background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document.
Gwen S Frazier	Gulf Power Company	3	Negative	The interpretation states “For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document.

Voter	Entity	Segment	Vote	Comment
Horace Stephen Williamson	Southern Company Services, Inc.	1	Negative	The interpretation states “For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document.
Leslie Sibert	Georgia Power Company	3	Negative	The interpretation states “For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard

Voter	Entity	Segment	Vote	Comment
				interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document.

Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access.

The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is

Voter	Entity	Segment	Vote	Comment
modified to eliminate the need for the interpretation.				
Paul Rocha	CenterPoint Energy	1	Negative	The SAR Drafting team indicated the FAQ document should not be relied upon for guidance in this case. CenterPoint Energy does not agree that an interpretation should replace previously published documents intended to guide entities in their compliance efforts. The disagreement between the FAQ document and the SAR Drafting team's interpretation creates confusion and therefore CenterPoint Energy must submit a negative vote.
Response: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation.				
Kim Warren	Independent Electricity System Operator	2	Negative	The scenario that WECC is concerned with presents a situation where it is quite likely that emergency support personnel would not be granted authorized access but would conduct their work using an account that has been authorized to the person who is required to escort or “supervise” the work being done under the account. The authorized owner of the account would be responsible, and in fact liable, for all activities that occur using that account. This places the onus on the account owner not the emergency support personnel which in turn places the requirement for training and PRA on the account owner not the emergency support personnel. The emergency support personnel are not being granted authorized access but are allowed the supervised use of an account that has been authorized to somebody else. NERC CIP-004-1 R2,R3 refer to authorized access as the determining factor for the requirement of training and Personnel Risk Assessment. As the situation for which WECC is seeking clarification contemplates a situation where, in all likelihood, authorized access would not be granted, therefore training and a PRA are not required. The interpretation that is presented does not contemplate this situation and therefore does not provide an

Voter	Entity	Segment	Vote	Comment
				appropriate or complete interpretation. It is suggested that the interpretation be revised to reflect the scenario as described.
Response: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.				
Gregory J Le Grave	Wisconsin Public Service Corp.	3	Negative	The standard should allow the escorted cyber access. It is the responsibility of the entity to assure that the escorting can detect malicious behavior. Failure to implement adequate controls would be a violation of the standard.
Response: The IDT is limited by the Guidelines for Interpretation Drafting Teams to clarify the meaning of the standard, not to expand the reach of the standard. While the IDT appreciates the comment, any change of the standard is outside the scope of the interpretation process.				
Anthony Jankowski	Wisconsin Energy Corp.	4	Negative	There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel.

Voter	Entity	Segment	Vote	Comment
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel.
Linda Horn	Wisconsin Electric Power Co.	5	Negative	There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel.
Response: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. Local assistance from support personnel must be managed as authorized cyber access, authorized unescorted physical access, or through visitor management programs, and this interpretation does not change requirements for compliance evidence.				
Greg Lange	Public Utility District No. 2 of Grant County	3	Negative	This interpretation does not answer the second part of Question one and therefore does not lend any clarity to the requested interpretation.
Response: Thank you for the comment. The interpretation language has been revised.				

Voter	Entity	Segment	Vote	Comment
Guy Andrews	Georgia System Operations Corporation	4	Negative	We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and

Voter	Entity	Segment	Vote	Comment
				FERC.
Harold Taylor, II	Georgia Transmission Corporation	1	Negative	We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential

Voter	Entity	Segment	Vote	Comment
				confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				
David Frank Ronk	Consumers Energy	4	Negative	We concur with the comments provided by ATC
Response: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				

Voter	Entity	Segment	Vote	Comment
Jason L Marshall	Midwest ISO, Inc.	2	Negative	We disagree with ignoring the FAQ that was developed by the standards drafting team. It gives insight into the intent of the SDT when developing the standard. The FAQ clearly considers cyber escorting possible. We do not think the drafting team should prevent creative solutions that may allow cyber escorting since the standard does not specifically exclude it. Further, the interpretation seems to imply that the background check must be completed prior to granting access. The standard is clear that any background checks can be completed up to 30 days after the access is granted.
Response: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation.				
Kathleen Goodman	ISO New England, Inc.	2	Negative	We disagree with the interpretation, as stated. The standard does allow for escorted/ supervised access to cyber assets for both logical and physical. However, if a company allowed external logical access the individual would need to meet the standard. If the individual is physically on site and is given logical access and is supervised by a qualified escort this is allowed. Therefore, we believe the Interpretation changes the existing Standard. Further, the statement by the SDT that "It is further noted that an FAQ is not a standard, and cannot create or dilute the language of the standard itself." seems to support the argument for expansion of the requirements since the FAQs, historically, have been used extensively by the industry to develop a voting position on Standards. This Interpretation appears to change the information the industry had available to it at the time the Standard was adopted.
Response: Thank you for your comment. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2,				

Voter	Entity	Segment	Vote	Comment
R3, and R4. The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation.				
Kirit S. Shah	Ameren Services	1	Negative	We do not agrre with the interpretation. With this interpretation if a Technician from a vendor was physically escorted inside the ESP he/she would not be allowed to work on any CCA's unless he had training and background check even though he is physically escorted. This could impact operations and potentially the operation of the BES.
Response: Thank you for the comment. The interpretation language has been revised. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.				
Dana Cabbell	Southern California Edison Co.	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct,

Voter	Entity	Segment	Vote	Comment
				unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Glen Reeves	Salt River Project	5	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct,

Voter	Entity	Segment	Vote	Comment
				unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Gregory Campoli	New York Independent System Operator	2	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, we disagree with the assertion that there is no way to provide effective supervision of cyber access to ensure actions do not harm the integrity of the Critical Cyber Asset or the reliability of the bulk power system. Finally, we are concerned about the reversal of previous NERC and FERC guidance. The interpretation does not directly answer the questions raised by WECC. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that is accomplished by an authorized individual working with the vendor in a supervising

Voter	Entity	Segment	Vote	Comment
				capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. We disagree with the assertion that there is no way to provide effective supervision of cyber access. There are tools available which can enable authorized personnel to provide temporary, indirect and monitored cyber access to personnel who have not been subjected to a personnel risk assessment and training. Furthermore, such tools can enable the supervising personnel to immediately revoke such access as needed. Therefore, we believe it is possible to provide supervised cyber access which can be controlled at least as effectively as escorted physical access. Finally, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Jerome Murray	Oregon Public Utility Commission	9	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
John Canavan	NorthWestern Energy	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
John T. Underhill	Salt River Project	3	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Keith V. Carman	Tri-State G & T Association Inc.	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
R Scott S. Barfield-McGinnis	Georgia System Operations Corporation	3	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Rick Spyker	AltaLink Management Ltd.	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems.

Voter	Entity	Segment	Vote	Comment
Robert Kondziolka	Salt River Project	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Ronald D. Schellberg	Idaho Power Company	1	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Terry L Baker	Platte River Power Authority	3	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Thomas J. Bradish	RRI Energy	5	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Thomas R. Glock	Arizona Public Service Co.	3	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
William Mitchell Chamberlain	California Energy Commission	9	Negative	We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.

Voter	Entity	Segment	Vote	Comment
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				
Kenneth R. Johnson	Public Utility District No. 1 of Chelan County	3	Negative	WECC comments apply
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				
Louise McCarren	Western Electricity Coordinating Council	10	Negative	WECC respectfully disagrees with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, WECC disagrees with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. WECC believes that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished

Voter	Entity	Segment	Vote	Comment
				only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. WECC is therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." WECC believes that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. WECC believes that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC.
Response: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ.				

Voter	Entity	Segment	Vote	Comment
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	While the SDT may have answered the questions, the response is not of the quality that can be used for reference and should be revised. There were two questions asked in this request for interpretation: 1. Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? 2. 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? The response to the first question was "The drafting team interprets that a vendor may be granted escorted physical access to Critical Cyber Assets; however, for a vendor to be granted authorized cyber access, the vendor must complete the risk assessment and training as required by CIP-004-1 Requirement R2." The response indicates that vendors must be authorized. Although not referenced directly it can be inferred that the response to the second questions was "....For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access....." This response is not framed well. If the inference is correct it appears to be consistent with Standard. The WECC interpretation is not consistent with the Standard. It is clear from the standards that no person can be granted permanent access and WECC is also correct that there is no standard provision for vendor temporary access except under an emergency. This does not change the response to the request for interpretation. The response is sound if it is true that there is no way to supervise cyber access as was Toni's response. "There is no such thing as escorted cyber access. I think careful reading of the standard supports that interpretation. " WECC's response in question is "We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity."

Response: Thank you for the comment. The interpretation language has been revised. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3,

Voter	Entity	Segment	Vote	Comment
and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendors providing temporary support.				