Individual or group. (39 Responses)
Name (25 Responses)
Organization (25 Responses)
Group Name (14 Responses)
Lead Contact (14 Responses)
Question 1 (38 Responses)
Question 1 Comments (39 Responses)
Question 2 (37 Responses)
Question 2 Comments (39 Responses)
Question 3 (37 Responses)
Question 3 Comments (39 Responses)

Individual
Keira Kazmerski
Xcel Energy
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
Jay Walker
NIPSCO
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Group
PacifiCorp
Sandra Shaffer
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Group
Southern Company
Shane Eaker
The request is asking for clarity on the application of a requirement.
The interpretation expands the reach of the standard.
No
Comments: Question 2 and 3 from the Request for Interpretation are not answered by the interpretation. The answers simply describe how the CIP standards do not address the questions being asked. The standards do not address the scenario contemplated by the line of questioning and

should be remanded to the CIP SDT to fix in version 5 of the standards. Comment: Vendor support personnel dispatched to the various generation sites are selected base upon their physical availability and the expertise required on the projects. It is a difficult task to provide ongoing training and background checks for every potential individual from numerous vendors supporting a variety of systems. It is near impossible to monitor the ongoing employment status of this large number of vendor personnel, to assure timely removal from the access control list, that will be required if implemented as discussed in the proposed interpretation. At present, vendor personnel supplying setup/support may work freely on pre-shipped non-installed systems. This trusted relationship should be extended, to similar individuals under escort at the equipment site. If the support function requires that changes be made to systems, having site personnel follow the direction of the vendor expert presents an increase potential for error, while adding marginal security benefits.
Individual
Ronnie Hoeinghaus
City of Garland
The request is asking for clarity on the application of a requirement.
No
Disagree with the concept of there being no escorted Cyber Access. If someone with authorized access is working with a vendor or contractor on an issue, the system is more secure than if you give him authorized access just because he has a PRA and has had CIP training. Take for example, Hector Xavier Monsegur, the notorious hacker known as Sabu and leader of LulzSec. Because of his cooperation and work with the FBI and other agencies, he may end up with his record cleansed or at least be able to put on a resume his work with the FBI. Eight years from now, a 7 year criminal background check could be clear. If a company were to utilize him for a short term issue, would the company be more secure with him being “escorted” or with him being issued authorized access and allowed free access. It is noted in your supporting comments that the standard requirements do not state specifically that escorted cyber access is permitted. On the other hand, the standard requirements do not have statements preventing escorted cyber access either. Which is more secure?
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Group
Northeast Power Coordinating Council
Guy Zito
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
Thad Ness
American Electric Power
The request is asking for clarity on the meaning of a requirement.

The interpretation does not expand the reach of the standard.
Yes
AEP agrees with the overall interpretation, but offers the following commentsand recommendations for improving the interpretation. Responses to Questions 1 and 2: The response provided for Q1 does not definitively answer the question that was posed. The question posed asks what the definition is for “authorized access”, while the response essentially states that one has this access by being on the proper list. It is not clear from the response how those on the authorized list were added to it, i.e. that those individuals met the necessary training, risk assessment, and access requirements. This might be made clearer if, rather than generally mentioning R2, R3, and R4, specifically stating what those requirements are. The response provided for Question 2 more adequately addresses Question 1 than does the response to Q1.
Individual
Randi Nyholm
Minnesota Power
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
The request is asking for clarity on the application of a requirement.
The clarification requested by WECC specifically states that the WECC RC seeks clarification on the definition of authorized access "as applied to temporary support from vendors."
The interpretation does not expand the reach of the standard.
Yes
The SPP RE agrees with the interpretation, noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent the escorted individual from overtly, covertly, or inadvertently causing harm. Granting direct cyber access to someone without authorized access inhibits the ability to perform the escort responsibilities and introduces risk. As noted in the interpretation, this is why the standard specifically makes a distinction regarding "authorized, unescorted" physical access. Technically, escorted cyber access is not feasible. The SPP RE agrees that "over the shoulder" viewing via a webinar or close proximity presence, while possibly subject to the entity’s CIP-003/R5 information protection program, does not constitute cyber access.
Individual
Greg Rowland
Duke Energy
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
Brian J Murphy
NextEra Energy Inc.
The request is asking for clarity on the application of a requirement.

Each of the three questions is asking whether a class of individuals (i.e., temporary vendors and supervisors of vendors) is required to comply with CIP-004 R2, R3 and R4. Thus, the questions are requesting specific confirmation whether one is or is out of compliance based on how these classes of individuals are addressed under CIP-004.
The interpretation expands the reach of the standard.
It could be viewed that the interpretation requested tends to expand the reach of CIP-004, given the lack of clarity in the answers. Thus, if this interpretation goes forward, it is recommended that that the following clearer and more to the point answers be substituted for the current answers, so there is no expanding of CIP-004 nor an elaboration on how the standard applies to particular facts: 1. WECC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors. Answer: The term authorized access as used in CIP-004 is not limited or qualified by any type or class of employees or vendors. Thus, all employees and vendors (who desire either physical or cyber access) without regard to whether they are temporary support or not must either: (1) be escorted by someone with authorized unescorted physical or authorized cyber access, as applicable or (2) have been granted authorized unescorted physical or authorized cyber access by meeting the requirements of R2 and R3. Thus, there is no exception for temporary support from vendors, and the term authorized access applies to them in the same manner it applies to any other class or type of employee or vendor. 2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Answer: Yes. The language of CIP-004 applies to all employees and vendors that desire unescorted physical or cyber access to Critical Cyber Assets without regard to whether or not the employee or vendor is supervised. 3. Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? Answer. See answer to question 2 – supervised vendors are not exempt from CIP-004-1, Requirements R2, R3, and R4, thus the remainder of the question is moot.
No
As written, this interpretation should either be dismissed as in appropriate or the answers re-written to be clearer and more responsive. See answers to question 1 and 2.
Group
Bonneville Power Administration
Chris Higgins
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
BPA believes that if the drafting team allowed for the concept of supervised cyber access, they would be expanding the scope CIP-004.
Yes
Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
The request is asking for clarity on the meaning of a requirement.
WECC has requested a clarification of the definition of “authorized access” to determine if vendor personnel who provide supervised temporary support to Responsible Entities, are subject to CIP-004 R2 through R4. This is a subject of great relevance to Ingleside Cogeneration LP as we require all of our vendors to maintain robust cyber security programs, but agree with WECC that a literal reading of CIP-004 may require dedicated agents from each. Critical vendors such as Cisco or GE do not support an operating model like this – and we would argue that their security training and personnel screening procedures are superior. This subject will become especially prevalent when CIP Version 5 takes effect and all Responsible Entities will be required to have a cyber policy that addresses Cyber System Access. We would like to see this complex issue addressed now, before some precedence is set that proves to be uneconomical or unviable.
The interpretation expands the reach of the standard.

The project team has chosen to differentiate between escorted physical access where a vendor performs a non-cyber activity (such as replacing parts) from one where a cyber connection has been made. Ingleside Cogeneration LP believes the project team has read in extra language into the requirement – and changed FERC's intent in Order 706 paragraph 432. That paragraph was cited by WECC in the original Request for Interpretation, and clearly acknowledges that supervised access is a real-life operational need under certain circumstances. If anything, the Commission brings up a good point about the qualifications of the escort, but it does not seem appropriate that the drafting team has completely ruled out supervised cyber access. Furthermore, by logical inference, if the Responsible Entity can demonstrate that they can supervise remote cyber access, then that should be allowed as well.
No
Ingleside Cogeneration LP believes that the interpretation is an overly-literal reading of CIP-004 and may hamper routine technical support processes with no demonstrable reduction in cyber-risk . The power and convenience of remote vendor maintenance may be unavailable to all but the largest utilities should costs rise because of it. Such a result will actually diminish BES reliability as access to highly competent technical support and maintenance personnel becomes restricted. There may be acceptable solutions, however. It would seem that a single cyber certification of vendors such as Cisco and GE could be referenced in thousands of individual security policies. Alternatively, the industry could provide a single generic cyber training package and employee background check method for vendors. We would hope that NERC takes a leadership position in resolving these complex issues. Lastly, the industry needs more direction than that provided in the circular response to the first question. The project team essentially states that the Responsible Entity must determine who has authorized access to their Critical Cyber Assets and include them on an access list. That list will then define authorized access – leaving the door open for a wide variety of resolutions.
Individual
.
.
Individual
Michael Falvo
Independent Electricity System Operator
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
Kim Koster
MidAmerican Energy Company
The request is asking for clarity on the application of a requirement.
The request is asking for clarification on the application of the term "authorized access" in order to determine how to comply in the situation of temporary vendor support.
The interpretation expands the reach of the standard.
WECC is seeking "clarification on the definition of 'authorized access.'"
No
The request is asking how to comply with one or more requirements in a specific situation with vendor support. Requests as to how to comply, per the Rules of Procedure, do not meet the valid criteria of an interpretation request. While we agree with the conclusion in the proposed response, the draft response restates information that already is in the standard.

Group
Dominion
Connie Lowe
The request is asking for clarity on the meaning of a requirement.
The interpretation expands the reach of the standard.
The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard.
No
The following Dominion responses are provided in order of the questions asked by WECC: 1. The interpretation that individuals on the list of personnel authorized for cyber or unescorted physical access to CCAs are subject to CIP-004-1 R2, R3 (with allowed restrictions), and R4 is appropriate. 2. CIP-004-1-R4 specifically addresses authorized access and does not state that “all cyber access to Critical Cyber Assets must be authorized”. CIP-004-1-R2 and CIP-004-1-R3 (with allowed restrictions) apply to "personnel having authorized cyber or authorized unescorted physical access". The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard. 3. The concept of "escorted electronic access" is absent from CIP-004-1. Absent a standard, it should be up to each Registered Entity to determine by internal policy whether or not escorted electronic access should be allowed.
Individual
Kirit Shah
Ameren
The request is asking for clarity on the meaning of a requirement.
The interpretation expands the reach of the standard.
No
The CIP-004 R4 IDT interpretation relies on incorrect logic in stating that Standard does not allow for escorted (supervised) cyber access to cyber assets solely because "unescorted cyber" is not explicitly included in the CIP-004 R4 "list". We agree with the idea put forth in the Requirement that anyone with unfettered cyber access is a potential danger and in like manner, so would anyone with unescorted physical access. However, the reason the Requirement does not require those with escorted cyber access to be listed is not because such access is somehow not contemplated or not permitted but rather because, like escorted physical access, these individuals, and their actions, are well monitored and controlled and do not need the extra care and handling that ensues from being on "The List" for those free to take independent action. The mere fact that they do not need further "handling" does not mean in any way that they do not exist or that this in not permitted. We are concerned that IDT is using a classic argument from the negative to imply something is impermissible on that such use is not contemplated merely because it is absent from a list of threat types that need to be addressed.
Individual
Jonathan Appelbaum
United Illuminating Company
The request is asking for clarity on the meaning of a requirement.
The interpretation expands the reach of the standard.
No
The Interpretation DT correctly states that CIP-004 R2 and R3 apply to individuals on a list

designating them with authorized cyber access or authorized unescorted physical access to Critical Cyber Assets. The Interpretation DT makes an error in stating that CIP-004 limits the type of cyber access to a Critical Cyber Assets to only authorized individuals, that is, there is no opportunity to implement supervised remote access via terminal session (i.e. Webex) to support personnel not on the authorized cyber access list. The Reliability standards do not provide a definitive statement of the types of access allowed to Critical Cyber Assets. The Standards only provide the program requirements for three types of access; authorized physical, escorted physical, and authorized cyber. By not providing a definitive list of the types of access the original Drafting team did not exclude the type of access under review in this interpretation, that is, supervised cyber access via terminal session. At the time the Reliability standards was approved the concept of supervised remote access was known. The Interpretation Drafting Team can only conclude that the original Standard Drafting Team did not list specific requirements for this type of access. The Interpretation Drafting Team cannot conclude that this type of access was prohibited. The fact that CIP-007 does not contain a specific unescorted cyber access provision is irrelevant. CIP-007 R5 requires technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Supervised access via Webex is not unauthorized system access. When terminal session access is utilized, the activity is tracked by the Company. R5 does not state all authorized user activity, the Interpretation drafting team is adding the word authorized in its response and is expanding the scope. This conclusion is more sensible for service vendors and SCADA system providers. The Interpretation Drafting Team's interpretation would require, as the requestor noted, large vendors (such as CISCO) to take every entities cyber training course and submit to multiple background checks. This would be compliance for compliance sake and not for security. The Interpretation should have stated that the names of authorized individuals are maintained on a list. These individuals are required to comply with CIP-004 R2 through R4. Supervisory Cyber Access via terminal session is not prohibited explicitly by the Standards and is therefore allowed. There are no additional Reliability requirements for such access beyond those described in Standards CIP-002 through CIP-009.
Individual
Jim Eckelkamp
Progress Energy
The request is asking for clarity on the meaning of a requirement.
The interpretation expands the reach of the standard.
No
Progress Energy disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or onsite cyber access). Registered Entities should be able to allow vendors providing support temporary, indirect, and monitored access to in scope NERC CIP assets via remote terminal sessions (Live Mtg, Webex, etc) (just as escorted physical access is allowed) without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. In addition, Registered Entities should be able to allow vendors providing onsite temporary support escorted cyber access without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. There are multiple NERC CIP support vendors that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard. This includes process control vendors not just IT vendors. Honeywell, GE, ABB, Siemens, Babcock and Wilcox, Emerson, GTE, Wood Group are all DCS vendors/tuners that may need to provide escorted cyber access at Progress Energy and throughout the industry. Not allowing for escorted cyber access could have adverse impacts to BES Reliability since some of this work is needed not only during emergencies but also for ongoing maintenance. Long term service agreements are in place with these vendors that have warranty implications that require escorted cyber support for various process control systems. Many Registered Entities rely on these vendors/tuners to provide their expertise in support of continual operations for proprietary systems and do not employ resources with these specialized skill sets.
Individual

Andrew Ginter
Waterfall Security Solutions
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
No
Unidirectional remote screen view products using hardware-enforced unidirectional communications or "data diodes" can securely show remote, unauthorized personnel the contents of screens on Critical Cyber Assets which are inside of an ESP. The technology allows remote personnel to watch and advise as authorized individuals carry out cyber access to those CCAs without introducing any risk that the remote personnel can directly influence the monitored CCAs in any way. This mechanism addresses WECC's concern regarding being "excessively burdened by limiting access to timely support." Since unidirectional remote screen view technology prevents the unauthorized observer from carrying out any direct cyber access, the unidirectional technology should have been identified in the interpretation as a legitimate form of supervised remote access.
Individual
Thomas Johnson
Salt River Project
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
No
As written we disagree with the IDT team's interpretation of CIP-004. We recognize CIP-004 does not include the concept of any words relating to "escorting" or "supervision" in the requirement language. However, the interpretation is not clearly defined and reaches the conclusion that escorted electronic access is prohibited because a formal electronic access escorting requirement is not defined. It appears this conclusion was based on the fact that CIP-006 clearly defines "escorted" or "supervised" physical access to cyber assets. We believe this type of assumption sets a bad precedent for future interpretations. Additionally we believe this interpretation won't allow emergent electronic access when needed. We believe there is little or no risk associated with allowing escorted access to a known contracted support vendor, when support is needed. In fact we believe prohibiting this type of access increases the risk level to the BES.
Individual
Andrew Gallo
Austin Energy
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
No
We believe NERC should acknowledge that "escorted" cyber access is legitimate. If one of our employees is monitoring the cyber activities of the escorted vendor, our employee could terminate the session if the vendor began to take inappropriate actions. This is akin to the situation for escorted physical access. As long as the person is escorted, if s/he begins to take inappropriate action, the escort can take appropriate responsive action.
Group
Pepco Holdings Inc & Affiliates
David Thorne
The request is asking for clarity on the application of a requirement.

The interpretation does not expand the reach of the standard.
No
It is understood why the SDT applied a strict interpretation which results in no change to the existing standard. The requested interpretation would have changed the meaning and reach of the standard. However there still remains a very serious real problem. There is a need to allow cyber access to a vendor on some sort of an emergency basis without meeting R2 and R3. The Impact Statement in the Request for Interpretation submitted by WECC is a very serious problem for many entities that could result in a high risk or serious system reliability problem.
Group
FirstEnergy
Sam Ciccone
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
No
There is an inherent flaw in the interpretation because it is based on an inactive standard CIP-004-1. The current effective standard is CIP-004-3 which differs in a significant way from CIP-004-1. Version 3 of this standard now allows exceptions in emergency situations as stated from the phrase “except in specified circumstances such as an emergency” which is included in R2.1 and R3. This specifically affects the answer to WECC’s third question. Remote and on-site cyber access should be allowed under supervision during emergency situations and it would be very difficult to assure that all personnel offering remote assistance in these situations were assessed per the requirements of CIP-004. A second inherent flaw is that the interpretation is based on an inactive standard CIP-006-1. The current effective standard CIP-006-3 expressly describes visitor supervision requirements. Per CIP-006-3, R1.6, visitors are required to be continuously escorted within Physical Security Perimeters. This revised requirement should be integrated into the answers to WECC’s second and third question. Therefore, we suggest the team revise the interpretation to only make reference to the current Version 3 standards, and add language in the interpretation that there are exceptions for emergency situations as specified by the entity per CIP-003 which requires details of those emergency situations.
Group
Tacoma Public Utilities
Kieth Morisette
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Agree with the standard as written in the WECC position paper
Individual
Patrick Brown
Essential Power, LLC
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
No
In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation. In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory

compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support. Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard. There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access.
Group
Kansas City Power & Light
Dean Larson
The request is asking for clarity on the application of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
John Seelke
PSEG (Public Service Enterprise Group)
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
The inability to provide Escorted Cyber Access through a web-conference (or otherwise), can be detrimental to the reliability of the BES as the time to troubleshoot cyber/networking issues can be extensive without letting the remote support personnel have access to the troubled device.
Individual
Christina Bigelow
Midwest ISO
The request is asking for clarity on the meaning of a requirement.
The request seeks clarification of the meaning of "authorized access." As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
The interpretation expands the reach of the standard.
MISO respectfully submits that, based on a literal reading of the plain language of CIP-004, the phrase "authorized access" is not part of the language of the requirement requested for interpretation. The use of a specific term not utilized in the requirement as well as the assignment of a specific meaning and obligations from the requirement at issue to such a term by the Interpretation Drafting Team ("IDT") in its Interpretation expands the reach of the standard.
No

MISO respectfully submits that the IDT's proposed Interpretation of the phrase “authorized access” is unsupported by the plain language of CIP-004. The phrase “authorized access,” which is the subject of the Interpretation, does not appear in CIP-004. Instead, the Standard uses the phrase “authorized cyber or authorized unescorted physical access.” MISO understands that the question posed by the requestor utilized the term “Authorized Access”, but respectfully submits that the IDT should have provided clarification specifically regarding authorized cyber access and authorized unescorted cyber access, which clarification would have resulted in entities ability to more directly apply the interpretation to its compliance efforts under CIP-004-1, R2. Moreover, the IDT’s explanation of “authorized access” merely refers back to the requirements associated with access without providing the requested clarification. As a result, MISO does not agree with the Interpretation as to the answer provided in response to Question 1. As to the proposed answers to Questions 2 and 3, MISO respectfully submits that, without the specific clarification requested under Question 1, the Interpretation’s conclusions are not sufficiently supported by the text of CIP-004.

Group

ISO/RTO Standards Review Committee

Gregory Campoli

The request is asking for clarity on the meaning of a requirement.

The interpretation does not expand the reach of the standard.

Yes

Individual

Ron Donahey

Tampa Electric Company

The request is asking for clarity on the meaning of a requirement.

The interpretation does not expand the reach of the standard.

Yes

Although we believe that the Interpretations Drafting Team has correctly provided the interpretation, we believe that the standard should be changed to provide a vehicle for emergency vendor access via cyber or physical escorting. The lack of the ability to provide this emergency access could be detrimental to the reliability of the grid and may force Entities into non-compliance to meet the emergency situation.

Group

ACES Power Marketing Collaborators

Jason Marshall

The request is asking for clarity on the meaning of a requirement.

The interpretation expands the reach of the standard.

Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines “authorized access’ by stating that an individual has “authorized access” if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated “authorized access” with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since Console access is almost

always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device.

No

This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus, maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. Three terms are defined or bounded outside the standards development process. These terms include: authorized access, cyber access and physical access. We will not repeat our arguments regarding this expansion of the standard here. They can be found in question 2. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary to the interpretation, most (probably all) registered entities have a formal process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed. We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert, software expert).

Group

MISO Standards Collaborators

Marie Knox

The request is asking for clarity on the application of a requirement.

The interpretation expands the reach of the standard.
We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access.
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Individual
Joe Doetzl
CRSI
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
No
The response to question 1 attempts to define authorized access. The definition, even if local to CIP-004, should be expanded to include an indication that authorized access indicates personnel with approval to access Critical Cyber Assets. The presence of a person's name on a maintained list could be in error and would not be an indication of authorized access.
Individual
Darryl Curtis
Oncor Electric Delivery Company
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes
Oncor Electric Delivery agrees with this interpretation. The interpretation provides greater clarity on how a Compliance Enforcement Agency (CEA) addresses “cyber access” which includes both physical and remote acc
Individual
DANA SHOWALTER
E.ON CLIMATE & RENEWABLES
The request is asking for clarity on the meaning of a requirement.
The interpretation does not expand the reach of the standard.
Yes