Individual or group. (39 Responses)
Name (27 Responses)
Organization (27 Responses)
Group Name (12 Responses)
Lead Contact (12 Responses)
Question 1 (34 Responses)
Question 1 Comments (39 Responses)
Question 2 (35 Responses)
Question 2 Comments (39 Responses)
Question 3 (38 Responses)
Question 3 Comments (39 Responses)

Individual
Glen Hattrup
Kansas City Power & Light
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
Please see response in Question 3 comments. Concerns regarding the expansion of the standard are expressed there.
No
The Response to Question 1 is acceptable and matches what I believe is the common interpretation. The Response to Question 2 is not acceptable and dramatically extends the reach of the Requirement and Standard. There are a number of problems with the second Response, including: “essential” has not been clarified or defined; the proposed answer dramatically increases the scope of equipment that must now be classified as Critical Cyber Assets; and there is a viral effect to the proposed answer that will place an unwarranted burden upon Responsible Entities. The initial issue with the response is that the word in question is used to explain its definition. Defining “essential” as “is used to perform a function essential” does not clarify the intent of the word. It is understandably difficult, if not impossible, to generate a prescriptive list of “essential” elements of Critical Assets due to the variances in the utility industry. Clarification regarding the intent of the requirement is still possible. Regrettably, this definition does nothing to reduce the subjectivity of the original Requirement. A Response that encouraged the Responsible Entity to outline a method or generate a set of characteristics in order to define “essential” for their operations would have been appropriate. While not auditable, it would provide clarity and guidance during the selection process. The proposed definition dramatically increases the scope of equipment and components that must now be considered as critical. The phrase “is used to perform a function” shifts the focus from the essential component to the tool being used to support the essential component. This shift is further reinforced by the last sentence of the proposed Response. For example, let’s consider Load Flow or Contingency Analysis to be critical or essential for the operation of an EMS. By the proposed Response, when the Transmission Planner accesses the EMS to perform a flow calculation or analysis, the workstation he uses to “perform the function essential to the operation of the” Critical Asset is now considered a Critical Cyber Asset. Previously, only the application server that hosted Load Flow or Contingency Analysis would have needed to be considered a CCA. This slope becomes quite slippery as we consider another example. Many modern EMS’s utilize commercial operating systems and / or relational databases. These systems host critical portions of the EMS application and are rightfully considered as Critical Cyber Assets. These systems also require a variety of ongoing maintenance which requires an administrator to manually perform some task. The reliable operation of the systems would be jeopardized if the maintenance tasks were not performed and can therefore be considered critical or essential functions. As in the previous example, the proposed Response now makes the System Administrators’ workstations Critical Cyber Assets. This expansion of scope leads to the final problem with the proposed Response. The viral aspect of the last sentence in the proposed Response will have disastrous consequences for the Responsible Entities and their access to Critical Assets. The sentence “Similarly any Cyber Asset, when used to perform…, becomes a Critical Cyber Asset” effectively draws in any system used to operate or maintain an essential function of the Critical Asset. This sentence

validates the previous two examples and the workstations in question becoming Critical Cyber Assets. Failure to limit the scope by considering control of BES assets or security pivot points opens any connecting system into consideration. We may attempt to mitigate this concern by placing workstations within the ESP, designating them as CCAs, and utilize them for maintenance or to perform other essential functions. However, the administrator or engineer must be physically at the workstation in order to perform their duties. Requiring physical presence will adversely affect overall BES reliability as critical personnel must travel to a particular physical location in order to perform their work. This will create delays that may allow operational problems to accelerate out of control. Remote access to these workstations would not be allowed because access from any other workstation would make the accessing workstation a Critical Cyber Asset as it again falls into the category of “any Cyber Asset, when used … becomes a Critical Cyber Asset.” The accessing workstation is essential to access the CCA maintenance workstation, therefore the accessing workstation is now a CCA as well. This illustrates the never-ending cycle of inclusion that has been created by the proposed Response. Assuming that prohibiting remote access is an acceptable outcome, there are other situations that may adversely affect the cyber security of the Critical Asset. Operating System security patches are frequently hosted on an external server. Having and delivering the security patch is essential for the reliable operation of the (operating) system. Does that external system (a cyber asset) now become a Critical Cyber Asset? Does the external asset that creates portable media containing the patches become Critical? It is not clear where the final line is drawn or if it can be. Auditing this expanded scope will be exceptionally difficult. The auditor will not be able to determine if all newly covered systems have been included in the compliance program. The Responsible Entity will likewise find enforcement exceptionally onerous or impossible. Extreme contortions will be required of otherwise normal, secure operational principles in order to comply. The proposed Response to Question 2 is unacceptable because it significantly increases the scope of the Requirement. In addition, as written, the proposed Response represents an enormous increase in compliance costs without a corresponding benefit for the Responsible Entity. Here is a suggested, alternative Response to Question 2. Any multi-component Critical Asset can be assumed to have two broad categories of components. There are components that are critical, or essential, to the operation of the asset and those that are optional. An essential component (or asset) of a Critical Asset may be defined as a component that would prevent the Critical Asset from operating as required by the Responsible Entity. Due to the wide variance within the industry, it is not possible for the Standard to prescriptively list what is essential or not. The Responsible Entity may find it beneficial to outline what would make a component essential or optional for their environment. Components supporting compliance with the Operational Standards for BES assets may be a good starting point for this outline. The Responsible Entity should seek to identify the core set of components required to operate the Critical Asset. This need not be an exhaustive list as one core component may have a cascade effect and force others to become critical by association. Capability of operation does not necessarily define a component as essential. Availability of other components capable of operation, intent, and / or operational precedence (primary, secondary components) should also be considered.
Individual
Warren Rust
Colorado Springs Utilities
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
the second part of Q2's response infers without justification that "operator-assisted remote control" is an essential function. Will NERC supply a list of cyber functions they consider essential to the operation of critical assets, or will they accept industry participants' self-determined answer to that question?
No
The Response to the RFI Q1 is appropriate & reasonable. The Response to Q2 (in short, “'essential to the operation of the Critical Asset' means '“essential to the operation of the Critical Asset'”) is circular and unhelpful. Additionally, the second part of Q2's response infers without justification that "operator-assisted remote control" is an essential function. Will NERC supply a list of cyber functions they consider essential to the operation of critical assets, or will they accept industry participants' self-determined answer to that question?

Individual
David Proebstel
PUD No.1 of Clallam County
The request is asking for clarity on the application of a requirement.
The request does not expand the reach of the standard.
Yes
The interpretation seems consistent and as long as the phrase "facilities utilized in monitoring and control" implies that both functions (monitoring and controlling) need to be utilized in order for the "systems and facilities" to be classed as a critical cyber asset. In other words, if the asset only monitors (and does not control) then it should fail the implied test.
Group
Northeastn Power Coordinating Council
Guy Zito
The request is asking for clarity on the meaning of a requirement.
Duke’s first question requests clarity on the meaning of the requirement. Duke’s second question requests clarity on the application of the requirement. I would have liked to check both boxes, but the program would only accept one box checked.
The request expands the reach of the standard.
The Interpretation expands the standard by referring to the human-to-machine interface. This interface is only a conduit to the CCA, it is not the CCA. It is assumed that the check boxes above refer to the interpretation, not the request.
No
We agree with the first response. We do not agree with the second response because: 1. It should not include an example. 2. The response should use the same wording for Critical Cyber Assets as the approved Glossary of Terms.
Group
Public Utilities Commission of Ohio Staff
Christopher Kotting, Energy Assurance
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
As noted below, it is our opinion that the Interpretation reduces the reach of the standard.
No
The Interpretation focuses on the use of Critical Cyber Assets, rather than the capabilities of those assets. By doing so, while the Interpretation does not address a potential gap, it creates a potential gap. The definition of a Critical Asset describes systems that if “destroyed, degraded or compromised” may influence the ability to maintain reliable operation of the grid. Based on the interpretation (particularly the response to Question 2), categories of equipment that may be capable of exerting control (and thus, if compromised could affect reliable operation of the grid) would be excluded from CIP treatment if they are not currently used for that purpose. For example, a laptop computer that had the necessary hardware and software to control SCADA systems, but operates in a backup position, or has some other primary use, might not have a negative impact if destroyed or degraded, but would potentially have a negative impact if compromised. In order to preserve the original intent, the word “used” in the Response to Question 2 should be replaced with “configured and equipped”. Duke is correct in its assertion that the issue of how CIP applies to portable hardware like laptop computers in the field clearly needs to be addressed, but this Interpretation is not the mechanism for doing so.
Group
Santee Cooper
Terry L. Blackwell

The request is asking for clarity on the application of a requirement.
The request does not expand the reach of the standard.
Yes
Individual
Martin Kaufman
ExxonMobil Research and Engineering
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
The response to question two does not clarify the meaning of the word 'essential' in the phrase 'essential to the operation of the critical asset'. The use of the word ‘essential’ in the interpretation's definition of ‘essential to the operation of the Critical Asset’ makes it difficult to understand the interpretation's author's explanation. In the example provided in the interpretaion, the critical asset can not be controlled or monitored (i.e. function properly) when an operator console’s Human Machine Interface is no longer operational. The example provided in the request for interpretation, remote access terminals (laptops), are not necessary for the operation for the critical asset, but they may be used to interface with the critical asset. The interpretation does not provide sufficient detail in the definition of ‘essential to the operation of the Critical Asset’ to determine if one or both of these examples qualify as cyber critical assets. The interpretation could better serve the industry by clarifying the definition of essential. Does 'essential' describe a piece of equipment that must function in order for the critical asset to properly operate or does essential describe a piece of equipment that may be used to operate the critical asset but it is not required for the proper operation of the critical asset?
Individual
Mark Simon
Encari, LLC
The request is asking for clarity on the application of a requirement.
The request does not expand the reach of the standard.
No
We disagree strongly with the Interpretation to Question #2. With respect to Question #2, the Interpretation provided is insufficient. By limiting critical cyber assets to those cyber assets that “perform a function essential to the operation of the Critical Asset…”, the interpretation excludes the possibility that "information" could constitute a critical cyber asset. Information, in and of itself, does not perform an essential function. Rather, information may support an essential operation or function of a critical asset. For example, if a critical asset is configured such that it cannot operate and support the reliability and operability of the Bulk-Power System without a real-time stream of data, that data fits the definition of a critical cyber asset, and should be protected. [Order 706, par. 271] In the CIP NOPR, the Federal Entergy Regulatory Commission (hereafter “FERC” or the “Commission”) noted that NERC’s definition of “cyber assets” includes “data.” The Commission stated that “marketing or other data essential to the proper operation of a critical asset, and possibly the computer systems that produce or process the data, would be considered critical cyber assets” subject to the CIP Reliability Standards. [CIP NOPR at P 114] Also, the Interpretation places an undue emphasis on the use of the word “perform.” Critical cyber assets do not always perform essential functions necessary to the operation of critical assets. Rather, they may control essential functions. For example, to the extent a critical cyber asset is involved in monitoring the grid through remote sensors, sounding alarms when grid conditions warrant, and operating equipment in field locations, that asset may not be performing

an essential function necessary to the operation of the critical asset, but may rather be controlling an essential function. Thus, the phrase "perform or control" should be substituted for the word "perform."
Individual
John Kutzer
John Kutzer
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
The response to Question 2 of the request for interpretation expands reach of the standards by not correctly identifying Critical Cyber Assets. The standard currently has two tests for an asset to be classified as a Critical Cyber Asset, the first being "essential to operation" (R3) and the second being the communication mechanism (R3.1, R3.2, & R3.3). The response to this question ignores the second criteria for identifying Critical Cyber Assets and as a result expands the reach of the standard.
No
The response to Question 1 is adequate. The response to Question 2 is not adequate. This response is circular, i.e. "essential is defined as essential". This response does not provide the clarification requested. Also, this response incorrectly states that "... any Cyber Asset, when used to perform a function essential to the operation of the Critical Asset, becomes a Critical Cyber Asset." This addresses only one aspect of the identification of a Critical Cyber Asset and expands the reach of the standard. Similarly,Compliance Application Notice — 0005, Compliance Application: CIP-002-3 R3 also incorrectly stated the requirements for identification of Critical Cyber Assets and effectively would expand the reach of the standard to any Cyber Asset "... with the capability and purpose of controlling Bulk Electric System assets remotely... should be designated as CCAs." Logically, this would imply that as a number of current smartphone models (e.g. iPhone, Blackberry, Android) as well as laptops, netbooks should now be designated as CCAs, as well as any other device that has this capability, thereby ignoring the requirements of the standard.
Group
Kansas City Power & Light
Joe Doetzl
The request is asking for clarity on the application of a requirement.
The request expands the reach of the standard.
No
The proposed interpretation infers a scope broader than the requirement stipulates. The question relates to the meaning of “essential to the operation of the Critical Asset” and it recommended to address the question with the first sentence of the interpretation and stop there. Recommend the interpretation as the following: The phrase “essential to the operation of the Critical Asset” means that the Critical Cyber Asset is used to perform a function essential to the operation of the Critical Asset”
Individual
Jennifer Rosario
Progress Energy
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
The sentence “For example, in a control center, a human-to-machine interface such as an operator console is used to perform the essential function of operator-assisted remote control” confuses the issue by describing the use of an operator console as “remote control”. Most would consider human-to-machine interfaces or operator consoles in control centers as primary control, not remote control. The question in the request for interpretation asks about laptops used for remote access. This answer, using the word “remote” in a different context than it is used in the question confuses the issue. It

implies (without saying it clearly) that the remote access laptop referred to in the question is essential to the operation of the control system, just as the human-to-machine interface is. The remote access laptop is not essential. It can be turned off and the control system will continue to function.
No
PGN agrees with the answer to Question 1, but not with the answer to Question 2. CIP-005 R2.4 allows “external interactive access” with proper controls. The confusing use of the term “remote control” as described in the comment above implies that any machine used for remote access becomes a Critical Cyber Asset, which PGN doesn’t believe is a valid interpretation. Cyber assets normally used to operate critical assets would be essential and classified as critical cyber assets as a result, however, a cyber device that is temporarily connected to a critical asset would be more like a piece of maintenance and test equipment (M&TE) and would be controlled as such - not as a critical cyber asset.
Individual
Martin Bauer
US Bureau of Reclamation
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
The answer to question 2 of the interpretation request did not add any clarity. The response merely restated the question as answer "essential to the operation of the Critical Asset” means that the Critical Cyber Asset is ... essential to the operation of the Critical Asset". Duke provided several clarifying points one of which was that essential can be viewed as “being incapable of removal without destroying the thing itself or its character.” which made the question: Does the term “essential to the operation of cyber asset” mean the cyber asset cannot be operated without the asset being evaluated? • When the response is “the Critical Cyber Asset is used to perform a function…” there is ambiguity in what the term “is” means in this context. Does it mean the CCA is used all the time…? Used sometimes…? That it can be used…? Illustrative of the issue is the situation where there are several control consoles distributed within a facility, any one of which can be employed to control an essential function associated with a CA. Are all the control consoles CCA? Can one of the consoles be designated as CCA and leave the other out? This question really isn’t clearly answered. This question can be answered very easily and quickly, but was not. This has implications down the road with relaying - if and when it becomes subject to the requirements as potential CCA. As an example, if there is a backup protective scheme meeting other criteria as CCA, will it be required to declare it a CCA because it might be used? • In a similar light to the first bullet, the response does not clearly address the “remote access” aspect of the query. What if something is tied to the system to support a temporary activity or need… How does this impact my CCA list and what are the obligations? An example here is the case where an entity is forced to deal with an emergency pandemic event which requires the entity to “remote in” to our system. Assume that this is an event was allowed for, but not something ever used. Is the entity required to have identified the remote console device they are now using as a CCA because it might one day be used to provide essential control features? Is the entity required to operate it from an environment that meets the Standards?
Group
Wisconsin Electric Power Company
Candace Morakinyo
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
The interpretation attempts to clarify the phrase "essential to the operation of the Critical Asset" by introducing a new concept of "perform a function essential to the operation of a Critical Asset". We believe that this fails to provide clarity, and instead expands the reach of the standard. The interpretation should focus on clarifying what the term "essential" means. Moreover, we believe that it is inappropriate to attempt to define "essential to the operation of the Critical Asset" by using the

term "essential" as this is a circular definition, and provides no new or useful information. We believe that "essential" cyber assets are those which are always required for operation of the Critical Asset; without which the primary mission (the qualities or attributes of an asset that causes it to be identified as 'Critical') of a Critical Asset cannot be performed.
No
Reference response to Question 2
Individual
Jonathan Appelbaum
United Illuminating
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
United Illuminating agrees with the response to Question 1. United Illuminating disagrees with the response to Question 2. The response utilizes the word essential to define essential. In essence NERC is stating that essential means essential. United Illuminating suggests that essential means those devices required by the asset to perform the functions that caused the asset to be identified as Critical.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
Yes
Individual
Darryl Curtis
Oncor Electric Delivery LLC
The request is asking for clarity on the application of a requirement.
The request does not expand the reach of the standard.
Yes
Individual
Eric Scott
Ameren
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
This interpretation does not clarify the phrase “essential to the operation of the Critical Asset” but introduces a new concept of “perform a function essential to the operation of a Critical Asset”. This interpretation fails to provide clarity, and instead expands the reach of this requirement.
No
This interpretation expands the scope of the requirement of the standard instead of providing clarity of what the phrase “essential to the operation of the Critical Asset” means. This interpretation should focus on clarifying what the term “essential” means.

Individual
John Brockhan
CenterPoint Energy
The request is asking for clarity on the meaning of a requirement.
No
CenterPoint Energy agrees with the response to Q1 but does not agree with the response to Q2 as it offers no additional clarity on the meaning of the phrase “essential to the operation of the Critical Asset”. CenterPoint Energy believes the interpretation should focus on the term “essential”. As indicated in Duke’s question, the term “essential” means “basic, vital, or fundamental”. CenterPoint Energy offers the following response to Duke’s Q2: If an entity has an asset that “may” be used to operate a Critical Asset, but is not "required" for operation of the Critical Asset, the asset would not be considered “essential to the operation of the Critical Asset”.
Individual
Andrew Pusztai
American Transmission Company
The request is asking for clarity on the meaning of a requirement.
None
The request expands the reach of the standard.
The interpretation attempts to clarify the phrase “essential to the operation of the Critical Asset” by introducing a new concept of “perform a function essential to the operation of a Critical Asset”. ATC believes that this fails to provide clarity, and instead expands the reach of the standard. The interpretation should focus on clarifying what the term “essential” means. Moreover, ATC believes that it is inappropriate to attempt to define “essential to the operation of the Critical Asset” by using the term “essential” as this is a circular definition, and provides no new or useful information. Finally, ATC believes that “essential” cyber assets are those which are always required for operation of the Critical Asset; without which the primary mission (the qualities or attributes of an asset that causes it to be deemed ‘Critical’) of a Critical Asset cannot be performed.
No
ATC is concerned with the response to Q #2 above and believes the language does not provide clarity or assistance to the industry on this important topic.
Individual
Joylyn Faust
Consumers Energy
The request does not expand the reach of the standard.
The response to the second, is at best circular and poorly written. Sentence one of this response is simply non responsive by way of being circular. Sentence one reads: "The phrase “essential to the operation of the Critical Asset” means that the Critical Cyber Asset is used to perform a function essential to the operation of the Critical Asset." To state that something is essential to operation means that it is used to perform a function essential to operation is a tautology, not a useful response. The response to the second request goes on to not address the remaining points raised by Duke.
Individual
Greg Rowland
Duke Energy
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
The interpretation of the standard seems to go beyond the reach of the standard. Need more

clarification on the “Essential” phrase in the standard.
No
The interpretation attempts to clarify the phrase “essential to the operation of the Critical Asset” by introducing the confusing concept of “perform a function essential to the operation of a Critical Asset”. We believe that this fails to provide clarity, and instead expands the reach of the standard. The interpretation should focus on clarifying what the term “essential” means. We believe that “essential” cyber assets are those which are always required for operation of the Critical Assets.
Individual
Kathleen Goodman
ISO New Enlgand Inc.
Cannot select both options; but the answer is both... Duke’s first question requests clarity on the meaning of the requirement. Duke’s second question requests clarity on the application of the requirement.
The request expands the reach of the standard.
The Interpretation expands the standard by referring to the human-to-machine interface. This interface is only a conduit to the CCA, it is not the CCA. It is assumed that the check boxes above refer to the interpretation, not the request.
No
We agree with the first response. We do not agree with the second response because: 1. It should not include an example 2. The response should use the same wording for Critical Cyber Assets as the approved Glossary of Terms.
Individual
Tony Kroskey
Brazos Electric Power Cooperative, Inc.
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
The response for Question 2 to provide clarity for the word essential uses the term essential. It did not provide clarity such as it means vital or cannot function without, etc.
Group
E.ON U.S.
Brent Ingebrigtson
No
The SDT interpretation of the phrase “essential to the operation of the Critical Asset” means that a “Critical Cyber Asset” is a cyber asset “used to perform a function essential to the operation of the Critical Assets”. E.ON U.S. does not believe that the proposed interpretation clarifies the standard. The issue posed by the request for interpretation is whether cyber assets used for remote support, such as laptops, would be considered “essential to the operation” of a Critical Asset, thus requiring application of CIP-006 physical controls to a laptop. Despite the obvious impracticality of applying CIP-006 controls to laptops, the interpretation leaves this question unanswered. As a result, the interpretation severely restricts the ability of entities to remotely support operations essential to the reliability of the BES. As a result, the reliability of the BES is eroded. The interpretation does nothing to address the questions posed. Recent guidance documents published by NERC concerning remote access are similarly unhelpful.
Group
MidAmerican Energy Company
Annette Johnston
The request is asking for clarity on the meaning of a requirement.

The request expands the reach of the standard.
The proposed interpretation does expand the reach of the standard. See question #3 comments.
No
We agree with the interpretation for Duke Energy’s Question #1. We do not agree with the interpretation for Duke Energy’s Question #2. The interpretation provided is circular, provides no new useful information, and potentially expands the reach of the standard which is not allowed for an interpretation. MidAmerican suggests the interpretation clarify “essential” in this context as cyber assets which “are always required” for the operation of the critical asset.
Individual
Matt Brewer
SDG&E
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
CIP002-R3 states “….the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset”. An asset that is “essential to the operation of the Critical Asset” is not the same as “any Cyber Asset used to perform a function essential to the operation of the Critical Asset”. There are many devices that could, in theory, be used to perform a function that would be considered essential to the operation of the Critical Asset that are not themselves essential to the operation of the Critical Asset. Essential should mean that an Entity is unable to operate the Critical Asset without that cyber asset (i.e. essential to the operation of the Critical Asset).
No
We believe there are actually two interpretations under project 2010-95. The first is regarding whether or not the examples in CIP003 R3 are prescriptive such that the types of assets meeting those descriptions must be assumed to be Critical Cyber Assets. We agree with NERC’s interpretation that the list is not meant to be prescriptive; rather it is a list of the types of assets that should be considered (evaluated). The second interpretation pertains to the definition of “essential” when referring to the standard’s language “essential to the operation of the Critical Asset”. CIP002-R3 states “….the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset”. An asset that is “essential to the operation of the Critical Asset” is not the same as “any Cyber Asset used to perform a function essential to the operation of the Critical Asset”. There are many devices that could, in theory, be used to perform a function that would be considered essential to the operation of the Critical Asset that are not themselves essential to the operation of the Critical Asset. Essential should mean that an Entity is unable to operate the Critical Asset without that cyber asset (i.e. essential to the operation of the Critical Asset).
Group
Bonneville Power Administration
Denise Koehn
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
YES, we agree with the response to question 1, that the “Examples…” are just that, examples, and not a prescriptive list. NO, the response to question 2 is inadequate. The phrase in question is used to define the phrase in question: “essential to the operation of the Critical Asset” means the device is used to perform a function “essential to the operation of the Critical Asset.” The example cited is good, but a definition of “essential,” as requested, is still needed.
Individual
Kasia Mihalchuk
Manitoba Hydro

Both. Question 1 seeks clarity of the examples in R3. Question 2 seeks clarity regarding the meaning of “essential to the operation of the Critical Asset”, and seeks clarity on the application of R3 in a given situation.
The request does not expand the reach of the standard.
Yes
Individual
Christine Hasha
ERCOT
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
ERCOT ISO agrees with the comments from the SRC. In addition, ERCOT ISO offers the following comments. The meaning of “essential” should be addressed more clearly with less emphasis on asset types (i.e.: operator consoles). The response confuses the issues addressed by the requestor. Another alternative to essential would be the use of the word “required”. Cyber Asset only becomes a Critical Cyber Asset if it is required to operate the Critical Asset. This would imply that the Critical Asset would not be able to perform the function required without the Critical Cyber Asset in question. Additionally, assets that are convenience or nice-to-have should be excluded from being categorized as Critical Cyber Assets.
Group
Electric Market Policy
Mike Garton
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
Dominion finds that the Response to Question 2 is both incomplete and confusing. To respond with “ ‘essential to the operation of the Critical Asset’ means … essential to the operation of the Critical Asset” does not answer the question. Specifically this response does not address the follow-on question about assets that “may” be used but are not “required”. The second and third sentences of the response to Question 2 leave more questions than provide answers. We agree that an HMI is essential (“indispensible, vital, fundamental, and necessary”) for “operator-assisted remote control”. However, in most cases, the HMI is not essential to the operation of the CA, since most if not all CAs can be operated manually and/or via protective devices (e.g., relays) locally. Finally, this response does not address remote access. Dominion believes that when several (not to be confused with redundant) solutions exist (e.g., multiple HMI workstations), that no single solution is essential. In question 2 Duke puts a statement about remote access, and Dominion agrees with Duke that remote access is valuable to operations. We believe remote access is addressed by CIP-005 and as such should not be addressed by CIP-002.
No
See comments in response to question 2. The interpretation is incomplete and in itself confusing and does not provide the clarity needed.
Individual
Thad Ness
American Electric Power
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
The last sentence in the second interpretation “Similarly, any Cyber Asset, when used to perform a

function essential to the operation of the Critical Asset, becomes a Critical Cyber Asset” needs to be removed or expanded to conform to the parameters of the requirement.
No
Comments: AEP is fine with the first interpretation, but the second needs additional work as we don’t feel it is responsive to the question asked and also expands upon the requirement as it excludes the sub-requirements that provide context of the definition of the critical cyber assets.
Individual
Jon Kapitz
Xcel Energy
No
The response to question 1 seems clear and adequate. The response to question 2 is inadequate in that it basically restates the phrase that had been questioned. It does not provide guidance for the question of assessing Cyber Assets that "may" be used but are not "required" and completely ignores the stated example of remote access.
Group
Edison Electric Institute
David Batz
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
No
For the Response to question 2, The interpretation attempts to clarify the phrase “essential to the operation of the Critical Asset” by introducing a new concept of “perform a function essential to the operation of a Critical Asset”. We believe that this fails to provide clarity, and instead expands the reach of the standard. The interpretation should focus on clarifying what the term “essential” means. Moreover, we believe that it is inappropriate to attempt to define “essential to the operation of the Critical Asset” by using the term “essential” as this is a circular definition, and provides no new or useful information. We believe that “essential” cyber assets are those which are always required for operation of the Critical Asset; without which the primary mission (the qualities or attributes of an asset that causes it to be deemed ‘Critical’) of a Critical Asset cannot be performed.
Individual
Jason Marshall
Midwest ISO
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
No
We agree with the answer to the first question. We disagree with the answer to the second question. “Essential to the operation of the Critical Asset” would mean that the Critical Asset cannot be operated without the Critical Cyber Asset or, at the very least, it would be challenging to operate the Critical Asset without the Critical Cyber Asset. One definition of essential as defined in Merriam-Webster dictionary is: “of the utmost importance”. Necessary and indispensable are common synonyms for essential identified in Merriam-Webster. Thus, a Cyber Asset only becomes a Critical Cyber Asset if it is necessary to operate the Critical Asset.
Individual
Dan Rochester
Independent Electricity System Operator
The request is asking for clarity on the meaning of a requirement.

It is not clear if this question is regarding the request or the response. In fact, the question “Do you believe this interpretation expands the reach of the standard?” conflicts with the two statements adjacent to the two checkboxes which refer to the ‘request’.
Yes
We agree with the response to Question 1. We agree with the intent of response to Question 2 but we believe (1) it should not include an example and (2) it could be worded more clearly. We respectfully suggested the following wording for the response to Question 2: The phrase “essential to the operation of the Critical Asset” means that the Critical Cyber Asset is used to perform a function fundamental to the operation of the Critical Asset. This means that; if the Critical Cyber Asset was not available or was severely impaired, the Critical Asset could not be operated or operation of the Critical Asset would be severely impaired.
Individual
Gregory Campoli
New York Independent System Operator
The request is asking for clarity on the meaning of a requirement.
Question #1 and #2 both seek to clarify the meaning of CIP-002-R3
The request does not expand the reach of the standard.
The request for interpretation seeks clarification on the meaning of CIP-002-3. The request for interpretation does not expand the reach of the standard. However, the current interpretation does expand the reach of the standard.
No
We do not agree with this interpretation due to concerns with the response to question #2. There are four issues with the response to question #2. First, the response does not directly answer the question asked. Second, the response repeats the same language as the original standard without further clarification. Third the example provided creates further confusion. Finally, the response expands the scope of the standard. The response does not directly answer question #2. A key element of this question is the second sentence which asks if cyber assets that “may” be used but are not “required” for operation of a Critical Asset must be considered “essential to the operation of the Critical Asset”. There is nothing in the response that clearly or directly addresses this basic question. The response attempts to clarify the meaning of the requirement by using the same language as the original requirement. If the phase “essential to the operation of the Critical Asset” is to mean something different than the defined NERC glossary terms and the dictionary definitions of the words contained therein then there should be other words used in the clarification aside from those already in the requirement. Expanding the phase to include the notion of a cyber asset performing a function “essential to the operation of the Critical Asset” does nothing to clarify the meaning of the phase “essential to the operation of the Critical Asset”. The example provided in the response creates additional confusion given the context of question #2. There are three sentences in question #2 each raising slightly different elements for consideration in the interpretation. A single example illustrating one situation where a cyber asset would be considered “essential to the operation of the Critical Asset” does little to clarify the different elements in question. In fact, the example may further confuse the meaning of the requirement by suggesting that this one example represents a pattern that must be applied to each element in question. Providing another example where a cyber asset would be determined not essential would enable people to compare and contrast the examples and may provide insight to the meaning of the requirement. The response to question #2 expands the scope of the standard. Given that the term “essential” is not defined in the NERC glossary, the dictionary definition is important. The Merriam –Webster dictionary definition, “ESSENTIAL implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character”, directly contradicts the notion that a cyber asset that is not “required” for operation of the Critical Asset must necessarily be considered “essential to the operation of the Critical Asset”. Therefore, this interpretation changes the meaning of the phase “essential to the operation of the Critical Asset” and effectively expands the scope of the standards to include cyber assets that may not otherwise be included.
Individual
Paul Crist

Lincoln Electric System
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
Yes
Group
Western Electricity Coordinating Council
Steve Rueckert
The request is asking for clarity on the meaning of a requirement.
The request does not expand the reach of the standard.
No
We agree that the first questions is answered adequatly and do not have any issues with the response provided. However, the the response to the second question used the word essential to try and define what is esential. It says that the phrase "essential to the operation of the Critical Asset" means it is used to perform a function "essential to the operation of the Critical Asset." We do not believe it is appropriate to use a term for which a definition is sought in the definition of the term.
Group
MRO's NERC Standards Review Subcommittee
Carol Gerou
The request is asking for clarity on the meaning of a requirement.
The request expands the reach of the standard.
No
We agree that the examples listed in CIP 002 R1 are not meant to be prescriptive. If they were prescriptive, all devices involved in “real-time inter-utility data exchange” would be considered Critical Cyber Assets (CCA), even if the data exchanged had no relevance to the operation of the BES. However, we believe that it is inappropriate to attempt to define “essential to the operation of the Critical Asset” by using the term “essential” as this is a circular definition, and provides no new or useful information. Also, this interpretation states that the Cyber Asset becomes a CCA “when used”. This may imply that the Cyber Asset, capable of performing an essential function, is not a CCA when not presently being used to perform the essential function. For example, a relief desk workstation, despite its present capability to execute controls on the BES would not be considered a CCA when not manned. Also, a standby EMS server would not be considered a CCA when not in use. Basing CCA classification on intermittent criteria such as “when used” may affect whether requirements, such as the need for a Recovery Plan, are also intermittent. We believe that “essential” cyber assets are those which are always required for operation of the Critical Asset; without which the primary mission (the qualities or attributes of an asset that causes it to be deemed ‘Critical’) of a Critical Asset cannot be performed.