UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)**	**Docket No. RD12-__-000**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF AN INTERPRETATION TO RELIABILITY STANDARD CIP-002-4 – CRITICAL CYBER ASSET IDENTIFICATION

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

August 1, 2012

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby requests the Federal Energy Regulatory Commission ("FERC" or "Commission") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of FERC's Regulations,[3] an interpretation of Reliability Standard CIP-002-4[4] — Critical Cyber Asset Identification, Requirement R3, to become effective concurrent with the date of a FERC Order approving this petition. The proposed interpretation is set forth in **Exhibit A** to this petition. Upon Commission approval of the interpretation, the standard will be referred to as CIP-002-4a — Critical Cyber Asset Identification.[5]

On January 31, 2010, Duke Energy requested a formal interpretation of CIP-002-1 Cyber Security – Critical Cyber Asset Identification, Requirement R3.[6] The NERC-assembled interpretation drafting team prepared the proposed response to the request for interpretation of Requirement R3 of CIP-002-4, which has been approved by the NERC

[1] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000 *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] 16 U.S.C. 824o (2006).

[3] 18 C.F.R. § 39.5 (2011).

[4] The proposed interpretation applies to versions 1, 2, 3, and 4 of the standard. For purposes of this filing, the standard will be referred to as CIP-002-4.

[5] The request for the interpretation for Requirement R3 of CIP-002-4 seeks clarity on what types of systems must be classified as Critical Cyber Assets and to provide clarity on the phrase "essential to the operation of the Critical Asset."

[6] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was in effect. The request was therefore processed referencing CIP-002. Subsequently, Versions 2, 3 and 4 of the CIP standards were approved by FERC. However, the changes in Versions 2, 3, and 4, relative to Version 1 of CIP-002, are not material to the substance of the interpretation request. Given that Version 3 is currently-effective, and Version 4 will become effective on April 1, 2014, NERC will append the requested interpretation to Version 3 or Version 4 of the CIP-002 standard, whichever is in effect at the time of FERC approval of this interpretation, in lieu of Version 1. *See Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009); *Order on Compliance*, 130 FERC ¶ 61,271 (2010) (March 31, 2010); *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (April 19, 2012).

Board of Trustees. No modification to the language contained in this specific Reliability Standard requirement is being proposed through the interpretation.

Exhibit A to this petition sets forth the interpretation of Requirement R3 to CIP-002-4. **Exhibit B** contains proposed Reliability Standard CIP-002-4a — Critical Cyber Asset Identification, which includes the appended interpretation of Requirement R3. **Exhibit C** to this petition contains the drafting team's consideration of industry comments for the interpretation to Requirement R3. **Exhibit D** contains the complete development history of the Interpretation of Requirement R3 of CIP-002-4. **Exhibit E** to this petition contains the roster of the interpretation drafting team that drafted the interpretation of Requirement R3. NERC is also filing this interpretation with applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[7]

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Charles A. Berardesco*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Holly A. Hawkins*
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips*
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[8] Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system, and with the duties of certifying an electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 states that all users, owners and operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

[7] Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[8] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (codified at 16 U.S.C. § 824o).

b. Basis for Approval of Proposed Reliability Standard Interpretation

The proposed interpretation is of a requirement contained within a Commission-approved Reliability Standard, but does not represent a new or modified Reliability Standard. However, the proposed Reliability Standard interpretation provides additional clarity with regard to the intent of the Reliability Standard. Therefore, NERC requests that the Commission approve the proposed interpretation.

c. Reliability Standards Development Procedure and Interpretation

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Standard Processes Manual*,[9] which is incorporated into the NERC Rules of Procedure as Appendix 3A.

A valid interpretation request is one that requests additional clarity about one or more requirements in a regulatory-approved Reliability Standard and does not request verification as to whether or not a specific approach will be judged as complying with one or more requirements in a regulatory-approved Reliability Standard. A valid interpretation in response to a request for interpretation provides additional clarity about one or more requirements within a Reliability Standard, but does not expand or limit the

[9] Note that FERC approved the new *Standard Processes Manual* in the Commission's *Order Approving Petition and Directing Compliance Filing*, 132 FERC ¶ 61,200 (2010), which replaced the NERC's *Reliability Standards Development Procedure Version 7* in its entirety. NERC developed these interpretations in accordance with the *Reliability Standards Development Procedure Version 7* until the *Standard Processes Manual* was approved on September 3, 2010. NERC's *Reliability Standards Development Procedure* is available on NERC's website at: http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf. The Standard Processes Manual available at: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf.

Reliability Standard or any of its requirements beyond the language contained in the standard.

The process for responding to a valid request for interpretation requires NERC to assemble a team with the relevant expertise to address the interpretation request. The interpretation drafting team is then required to draft a response to the request for interpretation and then present that response for industry ballot. If approved by the ballot pool and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed for approval by FERC and applicable governmental authorities in Canada. Then, when the affected Reliability Standard undergoes its next substantive revision, the interpretation will be incorporated into the Reliability Standard, as appropriate.

The proposed interpretation of Requirement R3 of CIP-002-4, as set out in **Exhibit A**, was approved by a ballot pool on April 30, 2012, with a weighted segment approval of 94.71 percent.[10] The proposed interpretation was approved by the NERC Board of Trustees on May 9, 2012.

IV. Proposed CIP-002-4a—Critical Cyber Asset Identification Interpretation

In Section IV(a), below, NERC summarizes the justification for the proposed interpretation of Requirement R3 of CIP-002-4, and explains the development of the interpretation. Section IV(b) summarizes the development proceedings for this

[10] The interpretation drafting team's considerations of comments for the interpretation of Requirement R3 is contained in **Exhibit C**. The complete development record for the interpretation, including the ballot pool, the final ballot results by registered ballot body members, stakeholder comments received during the balloting, and an explanation of how those comments were considered are set forth in **Exhibit D**.

interpretation and explains how stakeholder comments were addressed by the interpretation drafting team.

a. Justification for Approval of Interpretation

The stated purpose of CIP-002-4 is the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. Requirement R3 provides:

> **R3.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> **R3.1**. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> **R3.2** The Cyber Asset uses a routable protocol within a control center; or,
>
> **R3.3** The Cyber Asset is dial-up accessible.

In its interpretation request, Duke Energy sought clarification with respect to specific language in CIP-002-4, Requirement 3:

1. Is the phrase "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for

inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?

2. What does the phrase "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"?

In response to the Duke Energy request, the interpretation drafting team developed, and the industry stakeholders approved, the following interpretation:[11]

> The phrase "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
>
> The word "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset. A Cyber Asset that "may" be used, but is not "required" (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

As discussed below, the proposed interpretation of Requirement R3 of CIP-002-4 is consistent with the stated purpose of the Reliability Standard, which is to support the reliable operation of the Bulk Electric System by identifying and documenting Critical Cyber Assets associated with Critical Assets, because it ensures that assets that are essential to the operation of Critical Assets are subject to compliance with the standard.

[11] The interpretation drafting team was provided the guidelines for drafting interpretations in force at the time the interpretation was developed.

The first paragraph of the interpretation addresses the examples of Critical Cyber Assets that a Responsible Entity should consider during the identification and documentation process. The interpretation clarifies that the list of examples provided in Requirement R3 of CIP-002-4 are illustrative of the types of Cyber Assets that may be Critical Cyber Assets, and that the examples do not represent an exhaustive list of Critical Cyber Asset types.

Indeed, there are Critical Assets that are not included in the list of examples that could be identified by a Responsible Entity as Critical Cyber Assets, and there are Critical Assets that are included in the list of examples that may not otherwise meet the criteria for identification as Critical Cyber Assets. Therefore, the interpretation clarifies that the examples listed in Requirement R3 of CIP-002-4 are not prescriptive.

In the second paragraph, the proposed interpretation clarifies the meaning of the language "essential to the operation of the Critical Asset" in Requirement R3. Applying the common meaning of the word essential, the interpretation drafting team determined that the phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.[12] Applying the standard to these essential assets will ensure that Critical Cyber Assets associated with Critical Assets are properly identified and addressed by the standard.

Consistent with the purpose of Requirement R3, a Cyber Asset that "may" be used, but is not "required" for the operation of a Critical Asset, is clearly not "essential" to the operation of the Critical Asset. As such, Requirement R3 is intended to identify

[12] *See* Merriam-Webster's Dictionary (2012) (defining essential as: "1: of, relating to, or constituting essence: inherent.") available at: http://www.merriam-webster.com/dictionary/essential.

and document those Cyber Assets that are necessary for or inherent to the operation of the Critical Asset.

b. Summary of the Reliability Standard Development Proceedings

NERC presented the proposed interpretation of Requirement R3 for a first initial ballot from March 14, 2012, through March 23, 2012, and it achieved a quorum of 89.63 percent, with a weighted affirmative approval of 94.71 percent. There were seven negative ballots submitted in the initial ballot, and three of those included a comment, which initiated the need for a recirculation ballot.

A second draft interpretation was developed and posted for recirculation ballot from April 20, 2012, to April 30, 2012. Stakeholders supported the draft interpretation, which achieved a quorum of 92.68 percent with a weighted affirmative approval of 94.61 percent. There were 8 negative ballots submitted in the second initial ballot, and four of those ballots included a comment.

As demonstrated in the summary of comments presented below, a minority of commenters noted disagreement with certain aspects of the proposed interpretation, and some balloters commented on more than one issue. Specifically, reasons cited for negative ballots included the following:

- With respect to the response to Question 1, commenters disagreed that the types of Cyber Assets provided in the example "should be considered" and noted that the language "should be considered" is not found in CIP-002-3, Requirement R3, and should not be inferred. The interpretation drafting team explained, and a majority of commenters agree, however,

that the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, which requires some "consideration" within the context of the requirement.

- With respect to the response to Question 2, commenters stated that the interpretation could be construed as restricting the reach of the standard. The interpretation drafting team noted that the interpretation is consistent with the purpose of the standard, but also acknowledged that the proposed interpretation may be construed by the commenters as a restriction on their prior, different understanding of the reach of the standard.
- With respect to the response to Question 2, commenters stated that the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term, either in an interpretation or in the *NERC Glossary of Terms*. The interpretation drafting team disagreed because the proposed interpretation clarifies the meaning of "essential" as it applies to the purpose of this standard.

c. Future Action

The currently effective CIP-002-3 Reliability Standard was approved by the Commission on March 31, 2010.[13] Reliability Standard CIP-002-4 was approved by the Commission on April 19, 2012, and will become effective on April 1, 2014.[14] Upon Commission approval of the requested interpretation, the interpretation shall remain in

[13] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010).
[14] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

effect until such time as the interpretation can be incorporated into a future revision of the standard.

V. Conclusion

NERC respectfully requests that FERC approve the interpretation to FERC-approved Reliability Standard CIP-002-4 Cyber Security – Critical Cyber Asset Identification, Requirement R3, as set out in **Exhibit A**, in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC's regulations. NERC requests that this interpretation be made effective immediately upon issuance of FERC's order in this proceeding.

Respectfully submitted,

/s/ Willie L. Phillips
Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 1st day of August, 2012.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

Exhibit A

Interpretations of Requirement R3 of CIP-002-4 — Critical Cyber Asset Identification.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard

Date submitted: 1/31/10

Date revised version submitted: 7/22/10

Contact information for person requesting the interpretation:

Name: Kim Long

Organization: Duke Energy Corporation

Telephone: 704-382-7179

E-mail: kim.long@duke-energy.com

Identify the standard that needs clarification:

Standard Number (include version number): CIP-002-1

(example: PRC-001-1)

Standard Title: Cyber Security – Critical Cyber Asset Identification

Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement: CIP – 002-1, Requirement R3

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

Clarification needed:

With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following:

1. Is the phrase "***Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange"*** meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be *assessed* for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
2. What does the phrase, ***"essential to the operation of the Critical Asset"*** mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
    - *The term "essential" is not defined in the NERC Glossary. T*he Merriam –Webster dictionary provides the following definition of essential: "**ESSENTIAL** implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character." The dictionary provides the following synonyms for essential: "Inherent, basic, indispensible, vital, fundamental, and necessary."

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

If the phrase 'Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control' is meant to be prescriptive such that workstations, which are utilized in monitoring and control must be classified as Critical Cyber Assets, then the ability to provide remote support is not available to companies.

It is inherently not possible to implement all of the prescribed controls, i.e. CIP 006 physical controls, around workstations such as laptops when used from remote locations. The reliability of the Bulk Electric System will be eroded, rather than enhanced, if companies do not have the ability to remotely access the Critical Asset environment by utilizing laptop workstations with the cyber security controls prescribed in CIP 005.

Interpretation 2010-INT-05: Response to Request for an Interpretation of NERC Standard CIP-002-1 R3 for the Duke Energy Corporation

The following interpretation of NERC Standard CIP-002-1 Cyber Security — Critical Cyber Asset Identification was developed by a sub team of the Cyber Security Order 706 Standard Drafting Team.

Requirement Number and Text of Requirement

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a control center; or,
R3.3. The Cyber Asset is dial-up accessible.

Question 1

Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?

Response to Question 1

The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.

Question 2

What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the

Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.

Response to Question 2

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

Exhibit B

Proposed Reliability Standards CIP-002-3a and CIP-002-4a — Critical Cyber Asset Identification, that includes the appended interpretations of Requirement R3, submitted for approval.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3a

3. Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	Errata
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	December 16, 2009	Approved by the NERC Board of Trustees	Update
3a	May 9, 2012	Adopted by the NERC Board of Trustees	

Appendix 1

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
Response to Question 1
The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
Response to Question 2
The word “essential” is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the

well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “essential to the operation of the Critical Asset” means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that “may” be used, but is not “required” (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not “essential to the operation of the Critical Asset” for purposes of Requirement R3. Similarly, a Cyber Asset that is merely “valuable to” the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not “essential to the operation” of the Critical Asset.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~3~~3a

3. Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of

the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	Errata
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	December 16, 2009	Approved by the NERC Board of Trustees	Update
3a	May 9, 2012	Adopted by the NERC Board of Trustees	

Appendix 1

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
Response to Question 1
The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
Response to Question 2
The word “essential” is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the

well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “essential to the operation of the Critical Asset” means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that “may” be used, but is not “required” (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not “essential to the operation of the Critical Asset” for purposes of Requirement R3. Similarly, a Cyber Asset that is merely “valuable to” the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not “essential to the operation” of the Critical Asset.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4a

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	HIGH	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
R2	HIGH	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.
R3	LOWER	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	
4	4/19/12	FERC Order issued approving CIP-002-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
4a	May 9, 2012	Interpretation approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

Appendix 1[1]

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
Response to Question 1
The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
Response to Question 2

[1] In this version of the standard, the requirement at issue is R2 and the language has been modified. Question 1 in this interpretation no longer applies. Question 2 in the interpretation does apply to CIP-002-4 and therefore, the interpretation has been appended to this version of the standard.

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~4~~4a

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	HIGH	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
R2	HIGH	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.
R3	LOWER	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	
4	4/19/12	FERC Order issued approving CIP-002-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	
4a	May 9, 2012	Interpretation approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

Appendix 1[1]

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?
Response to Question 1
The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
Response to Question 2

[1] In this version of the standard, the requirement at issue is R2 and the language has been modified. Question 1 in this interpretation no longer applies. Question 2 in the interpretation does apply to CIP-002-4 and therefore, the interpretation has been appended to this version of the standard.

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

Exhibit C

Consideration of Comments for interpretation to Requirement R3 of CIP-002-4— Critical Cyber Asset Identification

Interpretation 2010-05
CIP-002-1 Requirement R3 for Duke Energy

Related Files

Status:
In May 2011 the Standards Committee appointed a standing CIP Interpretation Drafting team, and assigned this interpretation to that team. A parallel formal comment period and initial ballot ended March 23, 2012, and the team has posted its consideration of comments from that posting along with clean and redline versions of the interpretation, showing a minor clarifying change that was made in response to a comment.

Interpretation Process:
In accordance with the Reliability Standards Development Procedure, the interpretation must be posted for a 30-day pre-ballot review, and then balloted. There is no public comment period for an interpretation. Balloting will be conducted following the same method used for balloting standards. If the interpretation is approved by its ballot pool, then the interpretation will be appended to the standard and will become effective when adopted by the NERC Board of Trustees and approved by the applicable regulatory authorities. The interpretation will remain appended to the standard until the standard is revised through the normal standards development process. When the standard is revised, the clarifications provided by the interpretation will be incorporated into the revised standard.

Draft	Action	Dates	Results	Consideration of Comments
Interpretation of CIP-002-x R3 for Duke Energy Clean | Redline **Supporting Documents** CIP-002-3	Recirculation Ballot Info Vote>>	04/20/12 - 04/30/12	Summary Full Record	
Draft 2 Interpretation of CIP-002-x R3 for Duke Energy Clean| Redline to last posting **Supporting Documents** Unofficial Comment Form (Word)	Initial Ballot Updated Info(8) Vote>> Info(9)	03/14/12 - 03/23/12 (closed)	Summary Full Record	
	Formal Comment	02/08/12 -	Comments Received	Consideration of

CIP-002-3	Period Submit Comments>>	03/23/12 (closed)		Comments**(2)**
	Join Ballot Pool Join>>	02/08/12 - 03/08/12 (closed)		
Duke Interpretation of CIP-002-1 R3 Request for Interpretation	Formal Comment Period	09/08/10 - 10/08/10	Comments Received	Consideration of Comments**(1)**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Consideration of Comments on Interpretation of CIP-002-1 – Cyber Security – Critical Cyber Asset Identification, Requirement R3 for Duke Energy Corporation Project 2010-05

The CIP Interpretation Drafting Team thanks all commenters who submitted comments on the initial draft of an interpretation of CIP-002-1 — Cyber Security – Critical Cyber Asset Identification, Requirement R3 for Duke Energy Corporation. This interpretation was posted for a 30-day public comment period from September 8, 2010 through October 8, 2010. The stakeholders were asked to provide feedback on the interpretation through a special Electronic Comment Form. There were 39 sets of comments, including comments from more than 85 different people from approximately 75 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/Interp2010-05_Interpretation_CIP-002-1%20_Duke.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.

Index to Questions, Comments, and Responses

The Industry Segments are:

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

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1								
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10								
7.	Dean Ellis	Dynegy Generation	NPCC	5								
8.	Brian Evans-Mongeon	Utility Services	NPCC	8								
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5								
10	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5								
11	Kathleen Goodman	ISO - New England	NPCC	2								
12	Chantel Haswell	FPL Group, Inc.	NPCC	5								
13	David Kiguel	Hydro One Networks Inc.	NPCC	1								
14	Michael R. Lombardi	Northeast Utilities	NPCC	1								
15	Randy MacDonald	New Brunswick System Operator	NPCC	2								
16	Bruce Metruck	New York Power Authority	NPCC	6								
17	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10								
18	Robert Pellegrini	The United Illuminating Company	NPCC	1								
19	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1								
20	Saurabh Saksena	National Grid	NPCC	1								
21	Michael Schiavone	National Grid	NPCC	1								
22	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3								
			1	2	3	4	5	6	7	8	9	10

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2.	Individual	Christopher Kotting	Public Utilities Commission of Ohio Staff									x	

				1	2	3	4	5	6	7	8	9	10
3.	Group	Terry L. Blackwell	Santee Cooper	x		x			x				

	Additional Member	Additional Organization	Region	Segment Selection
1	S. Tom Abrams	Santee Cooper	SERC	1
2	Rene' Free	Santee Cooper	SERC	1

				1	2	3	4	5	6	7	8	9	10
4.	Group	Joe Doetzl	Kansas City Power & Light	x		x		x	x				

	Additional Member	Additional Organization	Region	Segment Selection
1	Michael Gammon	KCPL	SPP	1, 3, 5, 6

				1	2	3	4	5	6	7	8	9	10
5.	Group	Denise Koehn	Bonneville Power Administration	x		x		x	x				

	Additional Member	Additional Organization	Region	Segment Selection
1	Curt Wilkins	BPA, Transmission System Operations	WECC	1
2	BPA NERC CIP Team	BPA	WECC	1, 3, 5, 6

6.	Group	Mike Garton	Electric Market Policy	x		x		x	x				

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

	Additional Member	Additional Organization	Region	Segment Selection
1.		Michael Gildea	Dominion Resources Services, Inc	SERC 3
2.		Louis Slade	Dominion Resources Services, Inc.	SERC 6
3.		John Calder	Dominion Virginia Power	SERC 1
4.		Bruce Bingham	Dominion Resources Services, Inc.	SERC 5

7.	Group	Steve Rueckert	Western Electricity Coordinating Council										x

	Additional Member	Additional Organization	Region	Segment Selection
1.		Joshua Axelrod	WECC	WECC 10
2.		John Van Boxtel	WECC	WECC 10

8.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										x

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6
2.	Chuck Lawrence	American Transmission Company	MRO	1
3.	Tom Webb	WPS Corporation	MRO	3, 4, 5, 6
4.	Jason Marshall	Midwest ISO Inc.	MRO	2

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5. Jodi Jenson	Western Area Power Administration	MRO 1, 6										
6. Ken Goldsmith	Alliant Energy	MRO 4										
7. Alice Murdock	Xcel Energy	MRO 1, 3, 5, 6										
8. Dave Rudolph	Basin Electric Power Cooperative	MRO 1, 3, 5, 6										
9. Eric Ruskamp	Lincoln Electric System	MRO 1, 3, 5, 6										
10 Joseph Knight	Great River Energy	MRO 1, 3, 5, 6										
11 Joe DePoorter	Madison Gas & Electric	MRO 3, 4, 5, 6										
12 Scott Nickels	Rochester Public Utilties	MRO 4										
13 Terry Harbour	MidAmerican Energy Company	MRO 1, 3, 5, 6										
9. Individual	Candace Morakinyo	Wisconsin Electric Power Company			x	x	x	x				x
10. Individual	Brent Ingebrigtson	E.ON U.S.	x		x		x	x				
11. Individual	Annette Johnston	MidAmerican Energy Company	x				x					
12. Individual	David Batz	Edison Electric Institute	x				x					
13. Individual	Glen Hattrup	Kansas City Power & Light	x				x					
14. Individual	Warren Rust	Colorado Springs Utilities	x		x		x					
15. Individual	David Proebstel	PUD No.1 of Clallam County			x							
16. Individual	Martin Kaufman	ExxonMobil Research and Engineering	x				x		x			
17. Individual	Mark Simon	Encari, LLC	N/A									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Individual	John Kutzer	John Kutzer	N/A									
19.	Individual	Jennifer Rosario	Progress Energy	x		x		x		x			
20.	Individual	Martin Bauer	US Bureau of Reclamation					x					
21.	Individual	Jonathan Appelbaum	United Illuminating	x									
22.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	x		x		x	x				
23.	Individual	Darryl Curtis	Oncor Electric Delivery LLC	x									
24.	Individual	Eric Scott	Ameren	x		x		x	x				
25.	Individual	John Brockhan	CenterPoint Energy	x									
26.	Individual	Andrew Pusztai	American Transmission Company	x									
27.	Individual	Joylyn Faust	Consumers Energy			x	x	x					
28.	Individual	Greg Rowland	Duke Energy	x		x		x	x				
29.	Individual	Kathleen Goodman	ISO New Enlgand Inc.		x								
30.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	x				x					
31.	Individual	Matt Brewer	SDG&E	x		x		x					
32.	Individual	Kasia Mihalchuk	Manitoba Hydro	x		x		x					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Christine Hasha	ERCOT		x								
34.	Individual	Thad Ness	American Electric Power	x		x		x	x				
35.	Individual	Jon Kapitz	Xcel Energy	x		x		x	x				
36.	Individual	Jason Marshall	Midwest ISO		x								
37.	Individual	Dan Rochester	Independent Electricity System Operator		x								
38.	Individual	Gregory Campoli	New York Independent System Operator		x								
39.	Individual	Paul Crist	Lincoln Electric System	x		x		x					

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

Summary Consideration:

The interpretation drafting team ("IDT") thanks all who commented during the last posting of the interpretation for their interest and feedback. Commenters from the last posting of the interpretation provided constructive comments and concerns.
The interpretation drafting team agreed with the majority of the comments concerning the original interpretation of Question #1 and slightly modified the language to add clarity. The phrase "is illustrative, not prescriptive" was added to the response.
Question #2 was more challenging and there were disagreements between commenters whether interpreting "essential to the operation of the Critical Asset" expanded on the requirements of the standard or if common definitions could be used to make the interpretation.
In response to the comments received and reflective of the team's revisions to the interpretation, the interpretation drafting team carefully considered each comment and have provided responses to each comment.
Most commenters to Question #1 of the comment form indicated that they likely would have voted differently for each of the two responses to the questions in the Request for Interpretation. The IDT agrees that commenters should be able to respond separately to each question, and notes that it has changed the comment form accompanying the interpretation.

Organization	Yes or No	Question 1 Comment
Northeastn Power Coordinating Council	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.

Response: Thank you for your comment. The Interpretation Drafting Team agrees that Duke's first question is asking for clarity. The CIP interpretation Drafting Team modified the original response slightly by adding the phrase "is illustrative, not prescriptive."

Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical

Organization	Yes or No	Question 1 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each question.		
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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
Brazos Electric Power Cooperative, Inc.	The request is asking for clarity on the meaning of a requirement.	
SDG&E	The request is asking for clarity on the meaning of a requirement.	
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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original		

Organization	Yes or No	Question 1 Comment
response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
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
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	The request is asking for clarity on the meaning of a requirement.	
Electric Market Policy	The request is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Western Electricity Coordinating Council	The request is asking for clarity on the meaning of a requirement.	
MRO's NERC Standards Review Subcommittee	The request is asking for clarity on the meaning of a requirement.	
Wisconsin Electric Power Company	The request is asking for clarity on the meaning of a requirement.	
MidAmerican Energy Company	The request is asking for clarity on the meaning of a requirement.	
Edison Electric Institute	The request is asking for clarity on the meaning of a requirement.	
Kansas City Power & Light	The request is asking for clarity on the meaning of a requirement.	
Colorado Springs Utilities	The request is asking for clarity on the meaning of a requirement.	
PUD No.1 of Clallam County	The request is asking for clarity on the application of a requirement.	
ExxonMobil Research and	The request is asking for	

Organization	Yes or No	Question 1 Comment
Engineering	clarity on the meaning of a requirement.	
Encari, LLC	The request is asking for clarity on the application of a requirement.	
John Kutzer	The request is asking for clarity on the meaning of a requirement.	
Progress Energy	The request is asking for clarity on the meaning of a requirement.	
US Bureau of Reclamation	The request is asking for clarity on the meaning of a requirement.	
United Illuminating	The request is asking for clarity on the meaning of a requirement.	
South Carolina Electric and Gas	The request is asking for clarity on the meaning of a requirement.	
Oncor Electric Delivery LLC	The request is asking for clarity on the application of a requirement.	
Ameren	The request is asking for clarity on the meaning of	

Organization	Yes or No	Question 1 Comment
	a requirement.	
CenterPoint Energy	The request is asking for clarity on the meaning of a requirement.	
American Transmission Company	The request is asking for clarity on the meaning of a requirement.	None
Duke Energy	The request is asking for clarity on the meaning of a requirement.	
ERCOT	The request is asking for clarity on the meaning of a requirement.	
American Electric Power	The request is asking for clarity on the meaning of a requirement.	
Midwest ISO	The request is asking for clarity on the meaning of a requirement.	
Independent Electricity System Operator	The request is asking for clarity on the meaning of a requirement.	
Public Utilities Commission of Ohio Staff	The request is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Santee Cooper	The request is asking for clarity on the application of a requirement.	
Kansas City Power & Light	The request is asking for clarity on the application of a requirement.	
Bonneville Power Administration	The request is asking for clarity on the meaning of a requirement.	
Response: Thank you for your comment.		

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

Summary Consideration:

Many commenters expressed concern that the previously-posted interpretation, particularly the response to question #2 of the RFI, expanded or reduced the reach of the standard. In response, and after careful analysis and consideration of comments, the IDT has significantly changed the response to question #2 in a manner that it believes does not expand the reach of the requirement.

The second question from Duke Energy's RFI primarily asked for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke Energy's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Organization	Yes or No	Question 2 Comment
Northeastn Power Coordinating Council	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.

Response: Thank you for your comment. The IDT has clarified the question on the new comment form. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive."

Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
Public Utilities Commission of Ohio Staff	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.		
Electric Market Policy	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The application questions as to "how" the standard applies are beyond the scope of this Interpretation.		
Wisconsin Electric Power Company	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	The request expands the reach of the standard.	The proposed interpretation does expand the reach of the standard. See question #3 comments.
Kansas City Power & Light	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Colorado Springs Utilities	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?
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber		

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
John Kutzer	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." This interpretation singly addresses Duke's interpretation questions. The application discussion and applicability of the sub-requirements are beyond the scope of this interpretation.		
Progress Energy	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 2 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The application discussion is outside the scope of this interpretation.		
Ameren	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Transmission Company	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
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.
Response: Thank you for your comment. Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Duke Energy	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.
ISO New Enlgand Inc.	The request expands the reach of the	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.

Organization	Yes or No	Question 2 Comment
	standard.	
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
SDG&E	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).
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Electric Power	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Independent Electricity System Operator		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'.
Response: Thank you for your comment. The comment form will be revised.		
New York Independent System Operator	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.
Response: Thank you for your comment. The request for interpretation was for CIP-002-1. The same Requirement language is used in CIP-002 versions 1, 2 & 3. If approved, the interpretation will apply to all versions of CIP-002 in which the Requirement language for which the interpretation was requested persists. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber		

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	The request does not expand the reach of the standard.	
Brazos Electric Power Cooperative, Inc.	The request does not expand the reach of the standard.	
Midwest ISO	The request expands the reach of the standard.	
Manitoba Hydro	The request does not expand the reach of the standard.	
ERCOT	The request does not expand the reach of the standard.	
US Bureau of Reclamation	The request	

Organization	Yes or No	Question 2 Comment
	does not expand the reach of the standard.	
United Illuminating	The request does not expand the reach of the standard.	
South Carolina Electric and Gas	The request does not expand the reach of the standard.	
Oncor Electric Delivery LLC	The request does not expand the reach of the standard.	
PUD No.1 of Clallam County	The request does not expand the reach of the standard.	
ExxonMobil Research and Engineering	The request does not expand the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
Encari, LLC	The request does not expand the reach of the standard.	
Edison Electric Institute	The request expands the reach of the standard.	
Western Electricity Coordinating Council	The request does not expand the reach of the standard.	
MRO's NERC Standards Review Subcommittee	The request expands the reach of the standard.	
Santee Cooper	The request does not expand the reach of the standard.	
Kansas City Power & Light	The request expands the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
Bonneville Power Administration	The request does not expand the reach of the standard.	
Response: Thank you for your comment.		

3. Do you agree with this interpretation? If not, why not.

Summary Consideration:

Most commenters agreed with the response to Question #1 of the RFI, but disagreed with the response to Question #2; thus, most disagreed with the interpretation.

The CIP Interpretation Drafting Team agreed with the majority of the comments concerning the original interpretation of Question #1 and slightly modified the language to add clarity. The phrase "is illustrative, not prescriptive" was added to the response. Most commenters who did not agree with the interpretation did not agree with Question #2. The second question from Duke Energy's RFI primarily asked for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke Energy's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."

Several commenters asked for or provided observations concerning the application of the standard, and the drafting team responded that addressing "how" the standard should be applied was outside the scope of this interpretation.

Organization	Yes or No	Question 3 Comment
Northeastn Power Coordinating Council	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."		

Organization	Yes or No	Question 3 Comment
Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Public Utilities Commission of Ohio Staff	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." A discussion of applications of Critical Assets and Critical Cyber Assets is beyond the scope of this interpretation.		
Kansas City Power & Light	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

Organization	Yes or No	Question 3 Comment
		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"
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Bonneville Power Administration	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Electric Market Policy	No	See comments in response to question 2. The interpretation is incomplete and in itself confusing and does not provide the clarity needed.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 3 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
Western Electricity Coordinating Council	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.
Response: Thank you for your comment. The Interpretation Drafting Team (“IDT”) has modified the response to Question #1 slightly and it added the phrase “is illustrative, not prescriptive” to improve clarity. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
MRO's NERC Standards Review Subcommittee	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") has modified the response to Question #1 slightly and it added the phrase "is illustrative, not prescriptive" to improve clarity. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Wisconsin Electric Power Company	No	Reference response to Question 2
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
E.ON U.S.	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." Addressing application questions is beyond the scope of this interpretation.		
MidAmerican Energy Company	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 3 Comment
Edison Electric Institute	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Kansas City Power & Light	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

Organization	Yes or No	Question 3 Comment
		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,

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase “is illustrative, not prescriptive.” The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability		

Organization	Yes or No	Question 3 Comment
Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.” The discussion concerning application of the standard and examples of CAs and CCAs are beyond the scope of this interpretation.		
Colorado Springs Utilities	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?
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase “is illustrative, not prescriptive.” The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.” The question concerning NERC providing a list is beyond the scope of this interpretation.		
PUD No.1 of Clallam County	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to”		

Organization	Yes or No	Question 3 Comment
or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
ExxonMobil Research and Engineering	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?
Response: Thank you for your comment. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
Encari, LLC	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

Organization	Yes or No	Question 3 Comment
		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."
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The IDT's interpretation response to Question 2 is limited to clarifying the meaning of "essential to the operation of the Critical Asset," which could include a consideration of data as a Critical Cyber Asset.		
John Kutzer	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Progress Energy	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.
Response: Thank you for your comment. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical		

Organization	Yes or No	Question 3 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
US Bureau of Reclamation	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? o 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? o 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?
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical		

Organization	Yes or No	Question 3 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
United Illuminating	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Ameren	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
CenterPoint Energy	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

Organization	Yes or No	Question 3 Comment
		"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".
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Transmission Company	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Duke Energy	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.
Response: Thank you for your comment. Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the		

Organization	Yes or No	Question 3 Comment
operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
ISO New Enlgand Inc.	No	We agree with the first response. We do not agree with the second response because: 1. It should not include an example2. The response should use the same wording for Critical Cyber Assets as the approved Glossary of Terms.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Brazos Electric Power Cooperative, Inc.	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 3 Comment
SDG&E	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).
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive."The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
ERCOT	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 3 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Electric Power	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The sub-requirements are beyond the scope of this interpretation.		
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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3		

Organization	Yes or No	Question 3 Comment
works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Midwest ISO	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.
Independent Electricity System Operator	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
New York Independent System Operator	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3		

Organization	Yes or No	Question 3 Comment
works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	Yes	
South Carolina Electric and Gas	Yes	
Oncor Electric Delivery LLC	Yes	
Manitoba Hydro	Yes	
Santee Cooper	Yes	
Response: Thank you for your comment.		

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation 2010-INT-05
CIP-002-1 Requirement R3 for Duke Energy

The CIP-002-1 Requirement R3 Drafting Team thanks all commenters who submitted comments on Interpretation 2010-INT-05 CIP-002-1 Requirement R3 for Duke Energy. These standards were posted for a 45-day public comment period from February 8, 2012 through March 23, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 33 sets of comments, including comments from approximately 91 different people from approximately 58 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/2010-INT-05_Interpretation_CIP-002-1_Duke.html

Summary:

The IDT carefully reviewed all comments in response to the posting for parallel formal comment period and ballot that ended March 23, 2012. In the draft interpretation the IDT sought to clarify for Duke Energy that the examples given in CIP-002-x, Requirement R3 are illustrative, not prescriptive. The IDT also sought to clarify the meaning of the phrase "essential to the operation of the Critical Asset" as requested by Duke Energy, because the requirement specifies that "the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset." The IDT clarifies that a Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. The IDT made one clarifying change to reword a parenthetical phrase, and the IDT made no further changes to the interpretation. Many commenters agreed with the interpretation and several comments provided additional justification in support of the interpretation, and the IDT explains its rationale in response to several minority concerns below. The interpretation will be posted for a recirculation ballot.

- There were a few commenters that believe the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that in this case, it appears to be a question of semantics, where the IDT and industry both believe, overall, that the request is asking for clarity on the meaning of a requirement.
- Some commenters suggest that the interpretation could be construed as restricting the reach of the standard or that the interpretation is unnecessary or does not add new information, but the IDT disagrees. The IDT acknowledges that the interpretation may be construed to restrict many

parties or individuals' prior, different understanding or organizational interpretation of the reach of the standard. Furthermore, the interpretation is necessary because it provides clarity for all entities.

- A commenter disagreed with the interpretation by noting that the response to Question 1 states that the types of Cyber Assets in the example "should be considered," and the language "should be considered" is not found in CIP-002-3, Requirement R3 and should not be inferred. The IDT explains that the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, which requires some "consideration" within the context of the requirement.
- One commenter suggested that Version 4's language may have a similar issue. The IDT notes that an interpretation applies only so long as the relevant language in a standard is in effect, and it agrees that this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists.
- One commenter agreed with the Interpretation as to Question 2, but requested that the IDT clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". The commenter also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a Critical Asset. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, the IDT does agree that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct.
- Two commenters commented on the parenthetical clause in the original interpretation, suggesting that it was confusing upon first reading the language or that it seems to define "required." One commenter suggested rewording the clause, and one commenter suggested removing the clause as unnecessary. The IDT agrees, and it re-worded the clause from "(i.e. without which a Critical Asset cannot function as intended)" to, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)." This is a clarifying change, and it is not substantive.
- One commenter suggested that the IDT incorporate the provisions of NERC's CAN-0005 so that the CAN may be retired. The IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005.
- Other commenters were concerned that the interpretation does not explicitly state that redundancy is not a consideration for identifying Cyber Assets that are "essential." The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.

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

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

Index to Questions, Comments, and Responses

The Industry Segments are:

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

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

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

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

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

2.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

No additional members listed.

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

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

4.	Group	Christine Hasha	ISO/RTO Council Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Gary DeShazo	CAISO	WECC	2

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

3.	Steve Myers	ERCOT	ERCOT	2
4.	Ben Li	IESO	NPCC	2
5.	Kathleen Goodman	ISONE	NPCC	2
6.	Marie Knox	MISO	RFC	2
7.	Donald Weaver	NBSO	NPCC	2
8.	Greg Campoli	NYISO	NPCC	2
9.	Al DiCaprio	PJM	RFC	2
10.	Charles Yeung	SPP	SPP	2

5.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	5
3.	Louis Slade		RFC	5
4.	Michael Gildea		MRO	5

6.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hohlbaugh	FE	RFC	

7.	Group	Scott Harris	Kansas City Power & light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dean Larson	Kansas City Power & Light	SPP	1, 3, 5, 6
2.	Michael Gammon	Kansas City Power & Light	SPP	1, 3, 5, 6

8.	Group	Marie Knox	MISO Standards Collaborators								X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Cyrulewski	JDRJC Associates, LLC	RFC	8

9.	Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
2.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
3.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
4. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
5. Bob Solomon		Hoosier Energy	RFC 1										
10.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Mauricio Lopez	IID	WECC	1, 3, 4, 5, 6									
2.	Israel Gonzalez	IID	WECC	1, 3, 4, 5, 6									
3.	Peter Nguyen	IID	WECC	1, 3, 4, 5, 6									
11.	Individual	Brian Millard	Tennessee Valley Authority	X		X		X	X				
12.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
13.	Individual	Shane Eaker	Southern Company	X		X		X	X				
14.	Individual	Jay Walker	NIPSCO	X		X		X	X				
15.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
16.	Individual	Randi Nyholm	Minnesota Power	X		X		X	X				
17.	Individual	Thad Ness	American Electric Power	X		X		X	X				
18.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
19.	Individual	Michael Falvo	Independent Electricity System Operator		X								
20.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
21.	Individual	Kim Koster	MidAmerican Energy Company	X		X		X	X				
22.	Individual	Kirit Shah	Ameren	X		X		X	X				
23.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
24.	Individual	Thomas Johnson	Salt River Project	X		X		X	X				
25.	Individual	David Thorne	Pepco Holdings Inc	X		X							
26.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
27.	Individual	Patrick Brown	Essential Power, LLC	X				X					
28.	Individual	Anthony Jablonski	ReliabilityFirst										X
29.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
30.	Individual	Christina Bigelow	Midwest ISO		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
31.	Individual	Joe Doetzl	CRSI										
32.	Individual	Darryl Curtis	Oncor Electric Delivery Company	X									
33.	Individual	DANA SHOWALTER	E.ON CLIMATE & RENEWABLES					X					

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

☐ **The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.**

☐ **The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.**

Summary Consideration:

Most commenters agreed that question 1 of the request for interpretation is asking for clarity on the meaning of a requirement, and the IDT agrees. There were a few commenters that believe question 1 of the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that in this case, it appears to be a question of semantics, where the IDT and industry both believe, overall, that the request is asking for clarity on the meaning of a requirement.

Organization	Yes or No	Question 1 Comment
Southern Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	The question asks if the examples provided are prescribed to be CCAs or types of equipment that could be assessed as possible CCAs.
Response: Thanks for your comment and supporting rationale. This appears to be a question of semantics, where the IDT and industry majority believe, overall, that the request asks for clarity on the meaning of a requirement.		
Ingleside Cogeneration LP	The request in Question 1 of the Request for Interpretation is asking for clarity on the	Since the language and intent of a reliability requirement is the ultimate arbiter of compliance, examples may be considered by some auditors to be more than just "information only". Ingleside Cogeneration believes that the

Organization	Yes or No	Question 1 Comment
	application of a requirement.	request is looking to ensure that a violation will not be assessed because an example is not addressed by a Responsible Entity in the process of identifying its Critical Cyber Assets.
Response: Thanks for your comment and supporting rationale. This appears to be a question of semantics, where the IDT and industry majority believe, overall, that the request asks for clarity on the meaning of a requirement.		
Independent Electricity System Operator	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	
City of Austin dba Austin Energy	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	
MISO Standards Collaborators	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of whether the phrase at issue is illustrative or prescriptive. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thank you for your comment, which agrees with this IDT's position.		
Midwest ISO	The request in Question 1	The request seeks clarification of whether the phrase at issue

Organization	Yes or No	Question 1 Comment
	of the Request for Interpretation is asking for clarity on the meaning of a requirement.	is illustrative or prescriptive. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment and supporting rationale, which agrees with this IDT's position on the question.		
Northeast Power Coordinating Council	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Southwest Power Pool Regional Entity	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Bonneville Power Administration	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ISO/RTO Council Standards Review Committee	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Dominion	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
FirstEnergy	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Kansas City Power & light	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Imperial Irrigation District (IID)	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Tennessee Valley Authority	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
NIPSCO	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Transmission Company, LLC	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Minnesota Power	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Electric Power	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Duke Energy	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
MidAmerican Energy Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Ameren	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
United Illuminating Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Salt River Project	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Pepco Holdings Inc	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Essential Power, LLC	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ReliabilityFirst	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tampa Electric Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
CRSI	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Oncor Electric Delivery Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
E.ON CLIMATE & RENEWABLES	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

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

☐ **The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.**

☐ **The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.**

Summary Consideration:

Much like question 1, most commenters agree with the IDT that question 2 of the request for interpretation asks for clarity on the meaning of a requirement. Some commenters believe that the request asks for clarity on the application of a requirement, noting that the request asks if laptops at remote locations have to comply with CIP-002, Requirement R3. The IDT agrees that there may be an application component, but on balance, the request is asking for clarity. The IDT believes that the laptops illustration was provided as an example of why further clarity is needed in order to help the industry understand this requirement. One commenter asked whether the IDT believes the interpretation expands the scope of the requirement. The IDT does not.

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.	The request is asking for clarity on applying the requirement. The request is asking if laptops at remote locations have to comply with CIP-002 R3.
Response: Thanks for your comment and rationale, however the IDT believes that the laptops illustration was provided as an example of why further clarity is needed in order to help the industry understand this requirement.		
Salt River Project	The request in Question 2 of the Request for Interpretation is asking for	

Organization	Yes or No	Question 2 Comment
	clarity on the application of a requirement.	
City of Austin dba Austin Energy	The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.	
MISO Standards Collaborators	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in CIP-002. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Southern Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The question asks for clarification about the meaning of the word "essential."
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Ingleside Cogeneration LP	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	Question 2 revolves around the meaning of the term "essential" which determines if a Cyber Asset must be identified as a Critical Cyber Asset. This assessment becomes quite complex, especially in the case of mobile remote assets typically used in maintenance and trouble shooting. If CIP physical and electrical protections apply to such devices, some valuable capabilities will be lost. The NERC

Organization	Yes or No	Question 2 Comment
		Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?
Response: Thanks for your comment and provided rationale. The IDT views the remote laptops discussion as illustrative of why clarity needs to be provided surrounding the exact nature of this requirement. By rendering further clarity and then responding back to how it may affect that particular illustration, we have not substantively expanded the scope of the requirement.		
Midwest ISO	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in CIP-002. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Southwest Power Pool Regional Entity	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Bonneville Power	The request in Question 2 of	

Organization	Yes or No	Question 2 Comment
Administration	the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ISO/RTO Council Standards Review Committee	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Dominion	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
FirstEnergy	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Kansas City Power & light	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request in Question 2 of the Request for	

Organization	Yes or No	Question 2 Comment
	Interpretation is asking for clarity on the meaning of a requirement.	
Imperial Irrigation District (IID)	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tennessee Valley Authority	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
NIPSCO	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Transmission Company, LLC	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Minnesota Power	The request in Question 2 of the Request for Interpretation is asking for	

Organization	Yes or No	Question 2 Comment
	clarity on the meaning of a requirement.	
American Electric Power	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Duke Energy	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Independent Electricity System Operator	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Ameren	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
United Illuminating Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a	

Organization	Yes or No	Question 2 Comment
	requirement.	
Pepco Holdings Inc	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Essential Power, LLC	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ReliabilityFirst	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tampa Electric Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
CRSI	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 2 Comment
Oncor Electric Delivery Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
E.ON CLIMATE & RENEWABLES	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

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

☐ **The interpretation for Question 1 of the Request for Interpretation expands the reach of the standard.**

☐ **The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.**

Summary Consideration:

Many commenters agreed with the IDT's interpretation relating to Question 1 of the Request for Interpretation, noting agreement that the interpretation clarifies that the list of examples is illustrative, not prescriptive. Other commenters noted that the interpretation provides clarity and does not expand the reach of the standard. One commenter suggested that the interpretation introduces a concept not in the requirement, and references its explanation in comments provided in support of question 5 of this comment form. The IDT responds to this in response to consideration of comments for question 5.

Organization	Yes or No	Question 3 Comment
MISO Standards Collaborators	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Southern Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	The clarification that the examples are illustrative is helpful in understanding the requirement, but does not expand the reach of the requirement.

Organization	Yes or No	Question 3 Comment
Response: Thanks for your supporting comment.		
Midwest ISO	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Bonneville Power Administration	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ISO/RTO Council Standards Review Committee	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Dominion	The interpretation for Question 1 of the Request for Interpretation does	

Organization	Yes or No	Question 3 Comment
	not expand the reach of the standard.	
FirstEnergy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Kansas City Power & light	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ACES Power Marketing Standards Collaborators	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Imperial Irrigation District (IID)	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Tennessee Valley Authority	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of	

Organization	Yes or No	Question 3 Comment
	the standard.	
NIPSCO	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Minnesota Power	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Duke Energy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Independent Electricity System Operator	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Ingleside Cogeneration LP	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
MidAmerican Energy Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Ameren	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
United Illuminating Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Salt River Project	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Pepco Holdings Inc	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
City of Austin dba Austin Energy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Essential Power, LLC	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ReliabilityFirst	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Tampa Electric Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
CRSI	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
E.ON CLIMATE & RENEWABLES	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Southwest Power Pool Regional Entity	The interpretation for Question 1 of the Request for Interpretation expands the reach of the standard.	As discussed in our comments to Question #5 below, the interpretation for Question 1 introduces a concept not present in the currently approved requirement.

Organization	Yes or No	Question 3 Comment
Response: See IDT's response to Southwest Power Pool Regional Entity's Question #5 comments below.		

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

☐ **The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.**
☐ **The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.**

Summary Consideration:

Most commenters agree that the interpretation for question 2 of the Request for Interpretation does not expand the reach of the standard, but, rather, provides clarity around which Cyber Assets are essential compared to those that are merely valuable but not essential.

Some commenters suggest that the interpretation could be construed as restricting the reach of the standard, but the IDT disagrees. The IDT acknowledges that the interpretation may be construed to restrict many parties or individuals' prior, different understanding or organizational interpretation of the reach of the standard.

One commenter suggested the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term, either in an interpretation or in the NERC Glossary of Terms. The IDT observed that several definitions exist for this word, but it disagrees that the interpretation is unnecessary. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity relating to the Requirement itself.

Organization	Yes or No	Question 4 Comment
Southern Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	The response to question 2 does not expand the reach of the standard but provides clarity around which cyber assets are essential vs. assets that are valuable but not essential.

Organization	Yes or No	Question 4 Comment
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
ReliabilityFirst	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	The interpretation for Question 2 could be construed as restricting the reach of the standard.
Response: Thanks for your comment providing rationale. While the IDT disagrees that this interpretation restricts the original reach of this requirement, we do agree that it may be construed to restrict other parties' prior understanding or organizational interpretation of the reach of this requirement.		
Midwest ISO	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that a Critical Cyber Asset ("CCA") must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Southwest Power Pool Regional Entity	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the	

Organization	Yes or No	Question 4 Comment
	standard.	
Bonneville Power Administration	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
ISO/RTO Council Standards Review Committee	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Dominion	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
FirstEnergy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Kansas City Power & light	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
ACES Power Marketing Standards Collaborators	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Imperial Irrigation District (IID)	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Tennessee Valley Authority	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
NIPSCO	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Minnesota Power	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Duke Energy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Independent Electricity System Operator	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Ingleside Cogeneration LP	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Ameren	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
United Illuminating Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Salt River Project	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Pepco Holdings Inc	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
City of Austin dba Austin Energy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Essential Power, LLC	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Tampa Electric Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
CRSI	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
E.ON CLIMATE & RENEWABLES	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
MISO Standards	The interpretation for	MISO submits that, by clarifying that a Critical Cyber Asset ("CCA")

Organization	Yes or No	Question 4 Comment
Collaborators	Question 2 of the Request for Interpretation expands the reach of the standard.	must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MidAmerican Energy Company	The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.	The request is seeking the definition for the term "essential." Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms.
Response: Thanks for your comment and provided rationale. The IDT observed that several definitions exist for this word. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity to the Requirement itself.		

5. Do you agree with the Interpretation Drafting Team's response to *Question 1* of the Request for Interpretation? If not, please explain specifically what you disagree with.

Summary Consideration:

Most commenters agreed with the IDT's interpretation to question 1 of the Request for Interpretation. One commenter noted that guidance documents are often very long, and that one string of examples in the requirement could not be exhaustive. Furthermore, that commenter noted that the statement with the examples has been removed from CIP-002-4, presently pending FERC's approval, and that it seems apparent to that commenter that this action was taken because the examples only served to confuse Responsible Entities and auditors alike - and are more appropriately addressed in a guideline document. Both of those comments and rationales support the IDT's view that the list is illustrative, not prescriptive.

A commenter disagreed with the interpretation by noting that the response to Question 1 states that the types of Cyber Assets in the example "should be considered," and the language "should be considered" is not found in CIP-002-3, Requirement R3 and should not be inferred. The commenter agrees that the list of example Cyber Assets enumerated in Requirement R3 is not all inclusive, but notes that the list does identify types of Cyber Assets that perform functions that are essential to the operation of the control center. As such, the commenters suggests that examples are appropriately classified as Critical Cyber Assets *if* found in a control center that has been identified as a Critical Asset. In response, the IDT noted that the interpretation's response to Question 1 clarifies that the examples are illustrative. Thus, since it is not a prescriptive list, those examples "should be considered" to determine whether they meet the requirement's language. Since the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, some consideration is necessary within the context of the requirement.

One commenter agreed with the interpretation, but does not believe that the interpretation is necessary or adds new information. In response, the IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.

Organization	Yes or No	Question 5 Comment
Alberta Electric System Operator	Abstain	The AESO agrees with the interpretation of CIP-002, however we are casting an abstain vote as this standard is not applicable in Alberta at this time.

Organization	Yes or No	Question 5 Comment
Response: Thanks for providing the IDT with your rationale.		
Bonneville Power Administration	Affirmative	please refer to BPA's submitted comments
Brazos Electric Power Cooperative, Inc.	Affirmative	See comments submitted by ACES Power Marketing.
Consolidated Edison Co. of New York	Affirmative	See NPCC region-wide group comment form
FirstEnergy Corp.	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Southern Company Services, Inc.	Affirmative	See comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
California ISO	Affirmative	Comments provided jointly with the ISO/RTO Standards Review Committee
Electric Reliability Council of Texas, Inc.	Affirmative	ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee
AEP	Affirmative	Response is being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Alabama Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
FirstEnergy Energy Delivery	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Georgia Power Company	Affirmative	See electronic comments submitted by John Horishny.

Organization	Yes or No	Question 5 Comment
Gulf Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Mississippi Power	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form
Ohio Edison Company	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Wisconsin Energy Corp.	Affirmative	Comments are requested to be submitted using the separate electronic comment form rather than with the vote. I strongly support this interpretation and do not have any specific comments to submit with this vote.
AEP Service Corp.	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Bonneville Power Administration	Affirmative	Please see BPA comments submitted via the electronic comment form.
Brazos Electric Power Cooperative, Inc.	Affirmative	Please see comments filed by ACES Power Marketing.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Occidental Chemical	Affirmative	See comments by submitted by Ingleside Cogeneration LP
Southern Company Generation	Affirmative	Please see Southern Company comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
AEP Marketing	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of

Organization	Yes or No	Question 5 Comment
		American Electric Power.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period
Northern Indiana Public Service Co.	Affirmative	see NIPSCO comments submitted
Southern Company Generation and Energy Marketing	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
Bonneville Power Administration	Yes	BPA agrees that the examples in CIP-002 R3 are illustrative and not meant to be prescriptive.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MISO Standards Collaborators	Yes	MISO agrees with the Interpretation as to Question 1.
Response: The IDT recognizes this affirmation as limited only to Question 1		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP strongly agrees with the IDT's interpretation that the examples given in R3 should be considered "illustrative, not prescriptive". Our assessment shows two actions taken by NERC in regard to the requirement which support this clarification. First, the entire purpose of NERC's security guideline for "Identifying Critical Cyber Assets" is to provide a means for Responsible Entities to establish which Cyber Assets should be critical. This is a 47 page document with multiple evaluations and complex procedural steps. Clearly a single sentence in a requirement cannot be considered to be exhaustive - or anything more than a suggestion. Second, the statement with the examples has been removed from CIP-

Organization	Yes or No	Question 5 Comment
		002-4, presently pending FERC's approval. It seems apparent to us that this action was taken because the examples only served to confuse Responsible Entities and auditors alike - and are more appropriately addressed in a guideline document.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Tampa Electric Company	Yes	Tampa Electric agrees with the Interpretations Drafting Team response to Question 1
Response: The IDT recognizes this affirmation as limited only to Question 1		
Midwest ISO	Yes	MISO agrees with the Interpretation as to Question 1.
Response: The IDT recognizes this affirmation as limited only to Question 1		
Northeast Power Coordinating Council	Yes	
ISO/RTO Council Standards Review Committee	Yes	
Dominion	Yes	
FirstEnergy	Yes	
Kansas City Power & light	Yes	
ACES Power Marketing Standards Collaborators	Yes	
Imperial Irrigation District (IID)	Yes	
Tennessee Valley Authority	Yes	

Organization	Yes or No	Question 5 Comment
PacifiCorp	Yes	
Southern Company	Yes	
NIPSCO	Yes	
American Transmission Company, LLC	Yes	
Minnesota Power	Yes	
American Electric Power	Yes	
Duke Energy	Yes	
Independent Electricity System Operator	Yes	
Ameren	Yes	
United Illuminating Company	Yes	
Salt River Project	Yes	
Pepco Holdings Inc	Yes	
City of Austin dba Austin Energy	Yes	
Essential Power, LLC	Yes	

Organization	Yes or No	Question 5 Comment
ReliabilityFirst	Yes	
CRSI	Yes	
Oncor Electric Delivery Company	Yes	
E.ON CLIMATE & RENEWABLES	Yes	
MidAmerican Energy Co.	Negative	See MidAmerican comments
Southwest Power Pool Regional Entity	No	The response to Question 1 states that the examples of the types of Cyber Assets "should be considered." The language "should be considered" is not found in CIP-002/R3 and should not be inferred. While the SPP RE agrees that the list of example Cyber Assets enumerated in R3 is not all inclusive, the list does identify types of Cyber Assets that perform functions that are essential to the operation of the control center. As such, the examples are appropriately classified as Critical Cyber Assets *if* found in a control center that has been identified as a Critical Asset.
Response: Thanks for providing your rationale for response. The interpretation's response to Question 1 clarifies that the examples are illustrative. Thus, since it is not a prescriptive list, those examples "should be considered" to determine whether they meet the requirement's language. Since the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, some consideration is necessary within the context of the requirement.		
MidAmerican Energy Company	No	While we agree with the conclusion in the response to Question 1, we do not believe this interpretation is needed at this time. The response does not provide any new information.
Response: The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation		

Organization	Yes or No	Question 5 Comment
provides necessary clarity for all entities.		

6. Do you agree with the Interpretation Drafting Team's response to Question 2 of the Request for Interpretation? If not, why not.

Summary Consideration:

Most commenters agreed with the IDT's interpretation with respect to question 2 of the request for interpretation, and they agreed with the IDT's rationale that if a Cyber Asset is not required, but is merely "valuable to" the operation of a Critical Asset, it is not essential.

One commenter suggested that Version 4's language may have a similar issue. The IDT notes that an interpretation applies only so long as the relevant language in a standard is in effect, and it agrees that this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists.

One commenter agreed with the Interpretation as to Question 2, but requested that the IDT clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". The commenter also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a Critical Asset and therefore a Critical Cyber Asset pursuant to the clarification provided by the Interpretation. The commenter states that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct. As the majority of industry agreed with this balloted draft's current explanation of essential, the IDT did not incorporate the proposed change. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, the IDT does agree that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct.

Two commenters commented on the parenthetical clause in the original interpretation, suggesting that it was confusing upon first reading the language or that it seems to define "required." One commenter suggested rewording the clause, and one commenter suggested removing the clause as unnecessary. The IDT agrees, and it re-worded the clause from "(i.e. without which a Critical Asset cannot function as intended)" to, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)." This is a clarifying change, and it is not substantive.

One commenter suggested that the IDT incorporate the provisions of NERC's CAN-0005 so that the CAN may be retired. While the IDT understands this interpretation's rationale to be in keeping with CAN-0005 and possibly forthcoming CIP versions, the IDT is bound by the Guidelines for Interpretation Drafting teams to interpret the words on the page of any standard being interpreted. The IDT believes that incorporating the submitted suggestions would expand the scope of the requirement in question. Furthermore, the IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005.

Other commenters were concerned that the interpretation does not explicitly state that redundancy is not a consideration for identifying Cyber Assets that are "essential." The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.

One commenter suggested the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms. The IDT observed that several definitions exist for this word, but it disagrees that the interpretation is unnecessary. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity to the Requirement itself.

One commenter believed that the clarification provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, and that the interpretation does not provide additional clarity than what is provided in the existing guideline. The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.

Organization	Yes or No	Question 5 Comment
Alberta Electric System Operator	Abstain	The AESO agrees with the interpretation of CIP-002, however we are casting an abstain vote as this standard is not applicable in Alberta at this time.
Response: Thanks for providing the IDT with your rationale.		
Bonneville Power	Affirmative	please refer to BPA's submitted comments

Organization	Yes or No	Question 5 Comment
Administration		
Brazos Electric Power Cooperative, Inc.	Affirmative	See comments submitted by ACES Power Marketing.
Consolidated Edison Co. of New York	Affirmative	See NPCC region-wide group comment form
FirstEnergy Corp.	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Southern Company Services, Inc.	Affirmative	See comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
California ISO	Affirmative	Comments provided jointly with the ISO/RTO Standards Review Committee
Electric Reliability Council of Texas, Inc.	Affirmative	ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee
AEP	Affirmative	Response is being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Alabama Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
FirstEnergy Energy Delivery	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Georgia Power Company	Affirmative	See electronic comments submitted by John Horishny.
Gulf Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.

Organization	Yes or No	Question 5 Comment
Mississippi Power	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form
Ohio Edison Company	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Wisconsin Energy Corp.	Affirmative	Comments are requested to be submitted using the separate electronic comment form rather than with the vote. I strongly support this interpretation and do not have any specific comments to submit with this vote.
AEP Service Corp.	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Bonneville Power Administration	Affirmative	Please see BPA comments submitted via the electronic comment form.
Brazos Electric Power Cooperative, Inc.	Affirmative	Please see comments filed by ACES Power Marketing.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Occidental Chemical	Affirmative	See comments by submitted by Ingleside Cogeneration LP
Southern Company Generation	Affirmative	Please see Southern Company comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
AEP Marketing	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.

Organization	Yes or No	Question 5 Comment
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period
Northern Indiana Public Service Co.	Affirmative	see NIPSCO comments submitted
Southern Company Generation and Energy Marketing	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
Bonneville Power Administration	Yes	BPA agrees that if a Cyber Asset is not required, merely "valuable to" the operation of a Critical Asset, it is not essential.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
FirstEnergy	Yes	Since there are no question for general comments, we offer them in this last question.Just as a reminder, this Interpretation, once approve, will also need to be added to the pending CIP-002-4 standard which is currently before FERC for approval. It would seem that the Interpretation, if approved, could be added to the Version 4 standard as an errata change.
Response: Thanks for your additional comment. As an interpretation applies only so long as the relevant language in a standard is in effect, we agree this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists, which First Energy apparently believes to be the case.		
Kansas City Power & light	Yes	IDT clearly defines "essential" in its response. More importantly it states a "valuable" asset is not necessarily "essential" to the operatation of a Critical Asset, thereby, indirectly addressing Duke's concern with physical controls around workstations such as laptops when used from remote locations.

Organization	Yes or No	Question 5 Comment
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MISO Standards Collaborators	Yes	MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity's determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.
Response: Thanks for your provided rationale. As the majority of industry agreed with this balloted draft's current explanation of essential, we have not incorporated the proposed change. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, we agree with the MISO commenting body's final conclusion.		
ACES Power Marketing Standards Collaborators	Yes	While we agree with the drafting team, we recommend rewording "(i.e. without which a Critical Asset cannot function as intended)" to "(i.e. the Critical Asset cannot function without the Cyber Asset)". While the wording is technically correct, it is difficult to read and can be confusing.
Response: Thanks for your suggestion, which has been considered within the next draft. The IDT reworded the clause, but not the meaning or substance, so that it now reads, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)"		
Duke Energy	Yes	However, the interpretation could be improved by striking the parenthetical "(i.e., without which a Critical Asset cannot function as intended)," from the second paragraph. This parenthetical attempts to define the word "required", which is not necessary for the interpretation.
Response: Thanks for your suggestion, which has been considered within the next draft. Rather than remove it, the IDT reworded the clause, but not the meaning or substance, so that it now reads, "(i.e., a Critical Asset cannot function as intended without the		

Organization	Yes or No	Question 5 Comment
Cyber Asset)"		
Ingleside Cogeneration LP	Yes	We commend the Interpretation Drafting Team for developing a reading of the term "essential" based upon its commonly understood usage. We also agree that it is important to provide gradations which are close to the concept of essentiality, but does not meet the criticality litmus test. This allows the exclusion of Cyber Assets which "may be used, but not required" or are "merely valuable" to the inherent operation of the Critical Asset. It is left up to the Responsible Entity to make those assessments using an internal methodology that is comprehensive and defensible - and is consistent with the intent of CIP-002 as it is written today. We realize this flexibility may be limited in CIP version 5. However, those standards must still go through the vetting process; which will allow the industry to review, post comments, and vote upon any proposed changes.
Response: Thanks for support and supporting rationale for this interpretation.		
Tampa Electric Company	Yes	Tampa Electric agrees with the Interpretations Drafting Team response to Question 2. We strongly support the concept that essential to the operation of the Critical Asset means that it is necessary for the operation of that Critical Asset.
Response: Thanks for your strong support.		
Midwest ISO	Yes	MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity's determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.

Organization	Yes or No	Question 5 Comment
Response: Thanks for your provided rationale. As the majority of industry agreed with this balloted draft's current explanation of essential, we see a greater risk in accepting the proposed change compared to leaving the words as currently written. Further, we agree with the MISO commenting body's final conclusion.		
Northeast Power Coordinating Council	Yes	
ISO/RTO Council Standards Review Committee	Yes	
Dominion	Yes	
Imperial Irrigation District (IID)	Yes	
Tennessee Valley Authority	Yes	
PacifiCorp	Yes	
Southern Company	Yes	
NIPSCO	Yes	
American Transmission Company, LLC	Yes	
Minnesota Power	Yes	
American Electric Power	Yes	
Independent Electricity System Operator	Yes	

Organization	Yes or No	Question 5 Comment
Ameren	Yes	
United Illuminating Company	Yes	
Salt River Project	Yes	
Pepco Holdings Inc	Yes	
City of Austin dba Austin Energy	Yes	
Essential Power, LLC	Yes	
Oncor Electric Delivery Company	Yes	
E.ON CLIMATE & RENEWABLES	Yes	
MidAmerican Energy Co.	Negative	See MidAmerican comments
Southwest Power Pool Regional Entity	No	The response to Question 2 must be revised to specifically include the proviso that redundancy is NOT a consideration when determining if a Cyber Asset is "essential." Redundancy cannot be a consideration because, generally, vulnerability of the reduntant asset is the same as the primary asset's vulnerability. To achieve security you have to consider both primary and redundant assets. The interpretation must also incorporate the provisions of CAN-0005 in such a way as to make CAN-0005 no longer necessary.
Response: While the IDT understands this particular rationale to be more in keeping with CAN-0005 and possibly forth-coming CIP versions, the IDT is bound by the Guidelines for Interpretation Drafting teams to interpret the words on the page of any standard		

Organization	Yes or No	Question 5 Comment
being interpreted. The IDT believes that incorporating the submitted suggestions would expand the scope of the requirement in question. Furthermore, the IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005. **The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.**		
MidAmerican Energy Company	No	MidAmerican Energy does not believe this interpretation is needed at this time. The request is seeking the definition for the term "essential." Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms. The interpretation provides no new useful information and creates more confusion by introducing the new term "inherent to."
Response: The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities. The phrase "inherent to" in the interpretation is contextual and clarifying information, and the IDT disagrees that it is a new term.		
ReliabilityFirst	No	The Interpretation's "Response to Question 2" may render CIP-002-3 through CIP-009-3 non-functional. The statement, "A Cyber Asset that 'may' be used, but is not 'required' (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not 'essential to the operation of the Critical Asset' for purposes of Requirement R3" transforms CIP-002-3 R3 into a single point of failure analysis. Cyber systems used in the operation of the BES are designed so there is no single point of failure. Therefore, there would be no Critical Cyber Assets in the meaning stated by the "Response to Question 2."The Interpretation must be revised to make clear that any Cyber Asset, even if replicated locally or remotely, that, if damaged, lost or compromised, can have a negative impact on the reliable operation of the associated Critical Asset must be identified as a Critical Cyber Asset.
Response: The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this		

Organization	Yes or No	Question 5 Comment
interpretation does not change that notion.		
CRSI	No	The definition provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. The interpretation does not provide additional clarity than what is provided in the existing guideline.
Response: Thanks for your rationale. The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.		

END OF REPORT

Exhibit D

Complete Record of Development of the Interpretation of Requirement R3 of CIP-002-4 — Critical Cyber Asset Identification.

Interpretation 2010-05
CIP-002-1 Requirement R3 for Duke Energy

Related Files

Status:
In May 2011 the Standards Committee appointed a standing CIP Interpretation Drafting team, and assigned this interpretation to that team. A parallel formal comment period and initial ballot ended March 23, 2012, and the team has posted its consideration of comments from that posting along with clean and redline versions of the interpretation, showing a minor clarifying change that was made in response to a comment.

Interpretation Process:
In accordance with the Reliability Standards Development Procedure, the interpretation must be posted for a 30-day pre-ballot review, and then balloted. There is no public comment period for an interpretation. Balloting will be conducted following the same method used for balloting standards. If the interpretation is approved by its ballot pool, then the interpretation will be appended to the standard and will become effective when adopted by the NERC Board of Trustees and approved by the applicable regulatory authorities. The interpretation will remain appended to the standard until the standard is revised through the normal standards development process. When the standard is revised, the clarifications provided by the interpretation will be incorporated into the revised standard.

Draft	Action	Dates	Results	Consideration of Comments
Interpretation of CIP-002-x R3 for Duke Energy Clean(14) | Redline(15) **Supporting Documents** CIP-002-3(16)	Recirculation Ballot Info(17) Vote>>	04/20/12 - 04/30/12	Summary(18) Full Record(19)	
Draft 2 Interpretation of CIP-002-x R3 for Duke Energy Clean(4) | Redline to last posting(5) **Supporting Documents** Unofficial Comment Form (Word)(6)	Initial Ballot Updated Info(8) Vote>> Info(9)	03/14/12 - 03/23/12 (closed)	Summary(10) Full Record(11)	
	Formal Comment	02/08/12 -	Comments Received(12)	Consideration of

CIP-002-3**(7)**	Period Submit Comments>>	03/23/12 (closed)		Comments**(13)**
	Join Ballot Pool Join>>	02/08/12 - 03/08/12 (closed)		
Duke Interpretation of CIP-002-1 R3 Request for Interpretation**(1)**	Formal Comment Period	09/08/10 - 10/08/10	Comments Received**(2)**	Consideration of Comments**(3)**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

When completed, email this form to: maureen.long@nerc.net
For questions about this form or for assistance in completing the form, call Maureen Long at 813-468-5998.

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard
Date submitted: January 31, 2010 Date revised version submitted: July 22, 2010 Date accepted: July 27, 2010
Contact information for person requesting the interpretation:
Name: Kim Long
Organization: Duke Energy Corporation
Telephone: 704-382-7179
E-mail: kim.long@duke-energy.com
Identify the standard that needs clarification:
Standard Number (include version number): **CIP-002-1**
Standard Title: **Cyber Security – Critical Cyber Asset Identification**
Identify specifically what requirement needs clarification:
Requirement Number and Text of Requirement: CIP – 002 R3 R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: **R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, **R3.2.** The Cyber Asset uses a routable protocol within a control center; or, **R3.3.** The Cyber Asset is dial-up accessible. Clarification needed: With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following: 1. Is the phrase "**Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and**

control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be *assessed* for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?

2. What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
   - *The term "essential" is not defined in the NERC Glossary. T*he Merriam –Webster dictionary provides the following definition of essential: "**ESSENTIAL** implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character." The dictionary provides the following synonyms for essential: "Inherent, basic, indispensible, vital, fundamental, and necessary."

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

If the phrase 'Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control' is meant to be prescriptive such that workstations, which are utilized in monitoring and control must be classified as Critical Cyber Assets, then the ability to provide remote support is not available to companies.

It is inherently not possible to implement all of the prescribed controls, i.e. CIP 006 physical controls, around workstations such as laptops when used from remote locations. The reliability of the Bulk Electric System will be eroded, rather than enhanced, if companies do not have the ability to remotely access the Critical Asset environment by utilizing laptop workstations with the cyber security controls prescribed in CIP 005.

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Consideration of Comments on Interpretation of CIP-002-1 – Cyber Security – Critical Cyber Asset Identification, Requirement R3 for Duke Energy Corporation Project 2010-05

The CIP Interpretation Drafting Team thanks all commenters who submitted comments on the initial draft of an interpretation of CIP-002-1 — Cyber Security – Critical Cyber Asset Identification, Requirement R3 for Duke Energy Corporation. This interpretation was posted for a 30-day public comment period from September 8, 2010 through October 8, 2010. The stakeholders were asked to provide feedback on the interpretation through a special Electronic Comment Form. There were 39 sets of comments, including comments from more than 85 different people from approximately 75 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/Interp2010-05_Interpretation_CIP-002-1%20_Duke.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.

Index to Questions, Comments, and Responses

The Industry Segments are:

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

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1								
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10								
7.	Dean Ellis	Dynegy Generation	NPCC	5								
8.	Brian Evans-Mongeon	Utility Services	NPCC	8								
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5								
10	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5								
11	Kathleen Goodman	ISO - New England	NPCC	2								
12	Chantel Haswell	FPL Group, Inc.	NPCC	5								
13	David Kiguel	Hydro One Networks Inc.	NPCC	1								
14	Michael R. Lombardi	Northeast Utilities	NPCC	1								
15	Randy MacDonald	New Brunswick System Operator	NPCC	2								
16	Bruce Metruck	New York Power Authority	NPCC	6								
17	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10								
18	Robert Pellegrini	The United Illuminating Company	NPCC	1								
19	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1								
20	Saurabh Saksena	National Grid	NPCC	1								
21	Michael Schiavone	National Grid	NPCC	1								
22	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3								
			1	2	3	4	5	6	7	8	9	10

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2.	Individual	Christopher Kotting	Public Utilities Commission of Ohio Staff									x	

				1	2	3	4	5	6	7	8	9	10
3.	Group	Terry L. Blackwell	Santee Cooper	x		x			x				

	Additional Member	Additional Organization	Region	Segment Selection
1	S. Tom Abrams	Santee Cooper	SERC	1
2	Rene' Free	Santee Cooper	SERC	1

				1	2	3	4	5	6	7	8	9	10
4.	Group	Joe Doetzl	Kansas City Power & Light	x		x		x	x				

	Additional Member	Additional Organization	Region	Segment Selection
1	Michael Gammon	KCPL	SPP	1, 3, 5, 6

				1	2	3	4	5	6	7	8	9	10
5.	Group	Denise Koehn	Bonneville Power Administration	x		x		x	x				

	Additional Member	Additional Organization	Region	Segment Selection
1	Curt Wilkins	BPA, Transmission System Operations	WECC	1
2	BPA NERC CIP Team	BPA	WECC	1, 3, 5, 6

6.	Group	Mike Garton	Electric Market Policy	x		x		x	x				

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

	Additional Member	Additional Organization	Region	Segment Selection
1.		Michael Gildea	Dominion Resources Services, Inc	SERC 3
2.		Louis Slade	Dominion Resources Services, Inc.	SERC 6
3.		John Calder	Dominion Virginia Power	SERC 1
4.		Bruce Bingham	Dominion Resources Services, Inc.	SERC 5

7.	Group	Steve Rueckert	Western Electricity Coordinating Council										x

	Additional Member	Additional Organization	Region	Segment Selection
1.		Joshua Axelrod	WECC	WECC 10
2.		John Van Boxtel	WECC	WECC 10

8.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										x

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6
2.	Chuck Lawrence	American Transmission Company	MRO	1
3.	Tom Webb	WPS Corporation	MRO	3, 4, 5, 6
4.	Jason Marshall	Midwest ISO Inc.	MRO	2

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
5. Jodi Jenson	Western Area Power Administration	MRO 1, 6										
6. Ken Goldsmith	Alliant Energy	MRO 4										
7. Alice Murdock	Xcel Energy	MRO 1, 3, 5, 6										
8. Dave Rudolph	Basin Electric Power Cooperative	MRO 1, 3, 5, 6										
9. Eric Ruskamp	Lincoln Electric System	MRO 1, 3, 5, 6										
10 Joseph Knight	Great River Energy	MRO 1, 3, 5, 6										
11 Joe DePoorter	Madison Gas & Electric	MRO 3, 4, 5, 6										
12 Scott Nickels	Rochester Public Utilties	MRO 4										
13 Terry Harbour	MidAmerican Energy Company	MRO 1, 3, 5, 6										
9. Individual	Candace Morakinyo	Wisconsin Electric Power Company			x	x	x	x				x
10. Individual	Brent Ingebrigtson	E.ON U.S.	x		x		x	x				
11. Individual	Annette Johnston	MidAmerican Energy Company	x				x					
12. Individual	David Batz	Edison Electric Institute	x				x					
13. Individual	Glen Hattrup	Kansas City Power & Light	x				x					
14. Individual	Warren Rust	Colorado Springs Utilities	x		x		x					
15. Individual	David Proebstel	PUD No.1 of Clallam County			x							
16. Individual	Martin Kaufman	ExxonMobil Research and Engineering	x				x		x			
17. Individual	Mark Simon	Encari, LLC	N/A									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Individual	John Kutzer	John Kutzer	N/A									
19.	Individual	Jennifer Rosario	Progress Energy	x		x		x		x			
20.	Individual	Martin Bauer	US Bureau of Reclamation					x					
21.	Individual	Jonathan Appelbaum	United Illuminating	x									
22.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	x		x		x	x				
23.	Individual	Darryl Curtis	Oncor Electric Delivery LLC	x									
24.	Individual	Eric Scott	Ameren	x		x		x	x				
25.	Individual	John Brockhan	CenterPoint Energy	x									
26.	Individual	Andrew Pusztai	American Transmission Company	x									
27.	Individual	Joylyn Faust	Consumers Energy			x	x	x					
28.	Individual	Greg Rowland	Duke Energy	x		x		x	x				
29.	Individual	Kathleen Goodman	ISO New Enlgand Inc.		x								
30.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	x				x					
31.	Individual	Matt Brewer	SDG&E	x		x		x					
32.	Individual	Kasia Mihalchuk	Manitoba Hydro	x		x		x					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Christine Hasha	ERCOT		x								
34.	Individual	Thad Ness	American Electric Power	x		x		x	x				
35.	Individual	Jon Kapitz	Xcel Energy	x		x		x	x				
36.	Individual	Jason Marshall	Midwest ISO		x								
37.	Individual	Dan Rochester	Independent Electricity System Operator		x								
38.	Individual	Gregory Campoli	New York Independent System Operator		x								
39.	Individual	Paul Crist	Lincoln Electric System	x		x		x					

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

Summary Consideration:

The interpretation drafting team ("IDT") thanks all who commented during the last posting of the interpretation for their interest and feedback. Commenters from the last posting of the interpretation provided constructive comments and concerns.
The interpretation drafting team agreed with the majority of the comments concerning the original interpretation of Question #1 and slightly modified the language to add clarity. The phrase "is illustrative, not prescriptive" was added to the response.
Question #2 was more challenging and there were disagreements between commenters whether interpreting "essential to the operation of the Critical Asset" expanded on the requirements of the standard or if common definitions could be used to make the interpretation.
In response to the comments received and reflective of the team's revisions to the interpretation, the interpretation drafting team carefully considered each comment and have provided responses to each comment.
Most commenters to Question #1 of the comment form indicated that they likely would have voted differently for each of the two responses to the questions in the Request for Interpretation. The IDT agrees that commenters should be able to respond separately to each question, and notes that it has changed the comment form accompanying the interpretation.

Organization	Yes or No	Question 1 Comment
Northeastn Power Coordinating Council	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.

Response: Thank you for your comment. The Interpretation Drafting Team agrees that Duke's first question is asking for clarity. The CIP interpretation Drafting Team modified the original response slightly by adding the phrase "is illustrative, not prescriptive."

Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical

Organization	Yes or No	Question 1 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each question.		
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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
Brazos Electric Power Cooperative, Inc.	The request is asking for clarity on the meaning of a requirement.	
SDG&E	The request is asking for clarity on the meaning of a requirement.	
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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original		

Organization	Yes or No	Question 1 Comment
response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
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
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") agrees that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	The request is asking for clarity on the meaning of a requirement.	
Electric Market Policy	The request is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Western Electricity Coordinating Council	The request is asking for clarity on the meaning of a requirement.	
MRO's NERC Standards Review Subcommittee	The request is asking for clarity on the meaning of a requirement.	
Wisconsin Electric Power Company	The request is asking for clarity on the meaning of a requirement.	
MidAmerican Energy Company	The request is asking for clarity on the meaning of a requirement.	
Edison Electric Institute	The request is asking for clarity on the meaning of a requirement.	
Kansas City Power & Light	The request is asking for clarity on the meaning of a requirement.	
Colorado Springs Utilities	The request is asking for clarity on the meaning of a requirement.	
PUD No.1 of Clallam County	The request is asking for clarity on the application of a requirement.	
ExxonMobil Research and	The request is asking for	

Organization	Yes or No	Question 1 Comment
Engineering	clarity on the meaning of a requirement.	
Encari, LLC	The request is asking for clarity on the application of a requirement.	
John Kutzer	The request is asking for clarity on the meaning of a requirement.	
Progress Energy	The request is asking for clarity on the meaning of a requirement.	
US Bureau of Reclamation	The request is asking for clarity on the meaning of a requirement.	
United Illuminating	The request is asking for clarity on the meaning of a requirement.	
South Carolina Electric and Gas	The request is asking for clarity on the meaning of a requirement.	
Oncor Electric Delivery LLC	The request is asking for clarity on the application of a requirement.	
Ameren	The request is asking for clarity on the meaning of	

Organization	Yes or No	Question 1 Comment
	a requirement.	
CenterPoint Energy	The request is asking for clarity on the meaning of a requirement.	
American Transmission Company	The request is asking for clarity on the meaning of a requirement.	None
Duke Energy	The request is asking for clarity on the meaning of a requirement.	
ERCOT	The request is asking for clarity on the meaning of a requirement.	
American Electric Power	The request is asking for clarity on the meaning of a requirement.	
Midwest ISO	The request is asking for clarity on the meaning of a requirement.	
Independent Electricity System Operator	The request is asking for clarity on the meaning of a requirement.	
Public Utilities Commission of Ohio Staff	The request is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Santee Cooper	The request is asking for clarity on the application of a requirement.	
Kansas City Power & Light	The request is asking for clarity on the application of a requirement.	
Bonneville Power Administration	The request is asking for clarity on the meaning of a requirement.	
Response: Thank you for your comment.		

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

Summary Consideration:

Many commenters expressed concern that the previously-posted interpretation, particularly the response to question #2 of the RFI, expanded or reduced the reach of the standard. In response, and after careful analysis and consideration of comments, the IDT has significantly changed the response to question #2 in a manner that it believes does not expand the reach of the requirement.

The second question from Duke Energy's RFI primarily asked for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke Energy's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Organization	Yes or No	Question 2 Comment
Northeastn Power Coordinating Council	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.

Response: Thank you for your comment. The IDT has clarified the question on the new comment form. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive."

Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
Public Utilities Commission of Ohio Staff	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.		
Electric Market Policy	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The application questions as to "how" the standard applies are beyond the scope of this Interpretation.		
Wisconsin Electric Power Company	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	The request expands the reach of the standard.	The proposed interpretation does expand the reach of the standard. See question #3 comments.
Kansas City Power & Light	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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Colorado Springs Utilities	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?
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber		

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
John Kutzer	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." This interpretation singly addresses Duke's interpretation questions. The application discussion and applicability of the sub-requirements are beyond the scope of this interpretation.		
Progress Energy	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 2 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The application discussion is outside the scope of this interpretation.		
Ameren	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Transmission Company	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
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.
Response: Thank you for your comment. Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Duke Energy	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.
ISO New Enlgand Inc.	The request expands the reach of the	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.

Organization	Yes or No	Question 2 Comment
	standard.	
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The new comment form will provide two sets of boxes so you can provide a separate response to each interpretation response.		
SDG&E	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).
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Electric Power	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.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Independent Electricity System Operator		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'.
Response: Thank you for your comment. The comment form will be revised.		
New York Independent System Operator	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.
Response: Thank you for your comment. The request for interpretation was for CIP-002-1. The same Requirement language is used in CIP-002 versions 1, 2 & 3. If approved, the interpretation will apply to all versions of CIP-002 in which the Requirement language for which the interpretation was requested persists. The Interpretation Drafting Team ("IDT") believes that Duke's first question is asking for clarity. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber		

Organization	Yes or No	Question 2 Comment
Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	The request does not expand the reach of the standard.	
Brazos Electric Power Cooperative, Inc.	The request does not expand the reach of the standard.	
Midwest ISO	The request expands the reach of the standard.	
Manitoba Hydro	The request does not expand the reach of the standard.	
ERCOT	The request does not expand the reach of the standard.	
US Bureau of Reclamation	The request	

Organization	Yes or No	Question 2 Comment
	does not expand the reach of the standard.	
United Illuminating	The request does not expand the reach of the standard.	
South Carolina Electric and Gas	The request does not expand the reach of the standard.	
Oncor Electric Delivery LLC	The request does not expand the reach of the standard.	
PUD No.1 of Clallam County	The request does not expand the reach of the standard.	
ExxonMobil Research and Engineering	The request does not expand the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
Encari, LLC	The request does not expand the reach of the standard.	
Edison Electric Institute	The request expands the reach of the standard.	
Western Electricity Coordinating Council	The request does not expand the reach of the standard.	
MRO's NERC Standards Review Subcommittee	The request expands the reach of the standard.	
Santee Cooper	The request does not expand the reach of the standard.	
Kansas City Power & Light	The request expands the reach of the	

Organization	Yes or No	Question 2 Comment
	standard.	
Bonneville Power Administration	The request does not expand the reach of the standard.	
Response: Thank you for your comment.		

3. Do you agree with this interpretation? If not, why not.

Summary Consideration:

Most commenters agreed with the response to Question #1 of the RFI, but disagreed with the response to Question #2; thus, most disagreed with the interpretation.

The CIP Interpretation Drafting Team agreed with the majority of the comments concerning the original interpretation of Question #1 and slightly modified the language to add clarity. The phrase "is illustrative, not prescriptive" was added to the response. Most commenters who did not agree with the interpretation did not agree with Question #2. The second question from Duke Energy's RFI primarily asked for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke Energy's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."

Several commenters asked for or provided observations concerning the application of the standard, and the drafting team responded that addressing "how" the standard should be applied was outside the scope of this interpretation.

Organization	Yes or No	Question 3 Comment
Northeastn Power Coordinating Council	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset."		

Organization	Yes or No	Question 3 Comment
Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Public Utilities Commission of Ohio Staff	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." A discussion of applications of Critical Assets and Critical Cyber Assets is beyond the scope of this interpretation.		
Kansas City Power & Light	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

Organization	Yes or No	Question 3 Comment
		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"
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Bonneville Power Administration	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Electric Market Policy	No	See comments in response to question 2. The interpretation is incomplete and in itself confusing and does not provide the clarity needed.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 3 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
Western Electricity Coordinating Council	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.
Response: Thank you for your comment. The Interpretation Drafting Team (“IDT”) has modified the response to Question #1 slightly and it added the phrase “is illustrative, not prescriptive” to improve clarity. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
MRO's NERC Standards Review Subcommittee	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The Interpretation Drafting Team ("IDT") has modified the response to Question #1 slightly and it added the phrase "is illustrative, not prescriptive" to improve clarity. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Wisconsin Electric Power Company	No	Reference response to Question 2
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
E.ON U.S.	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." Addressing application questions is beyond the scope of this interpretation.		
MidAmerican Energy Company	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 3 Comment
Edison Electric Institute	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Kansas City Power & Light	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

Organization	Yes or No	Question 3 Comment
		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,

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase “is illustrative, not prescriptive.” The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability		

Organization	Yes or No	Question 3 Comment
Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.” The discussion concerning application of the standard and examples of CAs and CCAs are beyond the scope of this interpretation.		
Colorado Springs Utilities	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?
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase “is illustrative, not prescriptive.” The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.” The question concerning NERC providing a list is beyond the scope of this interpretation.		
PUD No.1 of Clallam County	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to”		

Organization	Yes or No	Question 3 Comment
or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
ExxonMobil Research and Engineering	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?
Response: Thank you for your comment. The IDT prepared a new response to Duke’s second question identifying that “essential” is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word “essential” implies “inherent to” or “necessary.” The phrase “inherent to or necessary to the operation of the Critical Asset” has the same meaning as “essential to the operation of the Critical Asset.” Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard’s Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets.”		
Encari, LLC	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

Organization	Yes or No	Question 3 Comment
		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."
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The IDT's interpretation response to Question 2 is limited to clarifying the meaning of "essential to the operation of the Critical Asset," which could include a consideration of data as a Critical Cyber Asset.		
John Kutzer	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Progress Energy	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.
Response: Thank you for your comment. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical		

Organization	Yes or No	Question 3 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
US Bureau of Reclamation	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? o 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? o 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?
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical		

Organization	Yes or No	Question 3 Comment
Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
United Illuminating	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Ameren	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
CenterPoint Energy	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

Organization	Yes or No	Question 3 Comment
		"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".
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Transmission Company	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Duke Energy	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.
Response: Thank you for your comment. Duke's second question is primarily asking for clarity on language in Requirement 3, "essential to the		

Organization	Yes or No	Question 3 Comment
operation of the Critical Asset." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
ISO New Enlgand Inc.	No	We agree with the first response. We do not agree with the second response because: 1. It should not include an example2. The response should use the same wording for Critical Cyber Assets as the approved Glossary of Terms.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Brazos Electric Power Cooperative, Inc.	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		

Organization	Yes or No	Question 3 Comment
SDG&E	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).
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive."The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
ERCOT	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.
Response: Thank you for your comment. The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the		

Organization	Yes or No	Question 3 Comment
Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
American Electric Power	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets." The sub-requirements are beyond the scope of this interpretation.		
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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3		

Organization	Yes or No	Question 3 Comment
works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Midwest ISO	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.
Independent Electricity System Operator	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.
Response: Thank you for your comment. The original response to Question 1 was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
New York Independent System Operator	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

Organization	Yes or No	Question 3 Comment
		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.
Response: Thank you for your comment. The original response was modified slightly by adding the phrase "is illustrative, not prescriptive." The IDT prepared a new response to Duke's second question identifying that "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. The well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "inherent to or necessary to the operation of the Critical Asset" has the same meaning as "essential to the operation of the Critical Asset." Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3		

Organization	Yes or No	Question 3 Comment
works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."		
Lincoln Electric System	Yes	
South Carolina Electric and Gas	Yes	
Oncor Electric Delivery LLC	Yes	
Manitoba Hydro	Yes	
Santee Cooper	Yes	
Response: Thank you for your comment.		

END OF REPORT

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-1a

3. Purpose: NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-002:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: June 1, 2006

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06
1a	TBD	Added Appendix 1 Interpreations	TBD

Appendix 1

Requirement Number and Text of Requirement
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.
Question 1
Is the phrase "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
Response to Question 1
The phrase "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.
Question 2
What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.

Response to Question 2
The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset. A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard

Date submitted: 1/31/10

Date revised version submitted: 7/22/10

Contact information for person requesting the interpretation:

Name: Kim Long

Organization: Duke Energy Corporation

Telephone: 704-382-7179

E-mail: kim.long@duke-energy.com

Identify the standard that needs clarification:

Standard Number (include version number): CIP-002-1

(example: PRC-001-1)

Standard Title: Cyber Security – Critical Cyber Asset Identification

Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement: CIP – 002-1, Requirement R3

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

Clarification needed:

With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following:

1. Is the phrase "***Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange"*** meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be *assessed* for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
2. What does the phrase, ***"essential to the operation of the Critical Asset"*** mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
    - *The term "essential" is not defined in the NERC Glossary. T*he Merriam –Webster dictionary provides the following definition of essential: "**ESSENTIAL** implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character." The dictionary provides the following synonyms for essential: "Inherent, basic, indispensible, vital, fundamental, and necessary."

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

If the phrase 'Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control' is meant to be prescriptive such that workstations, which are utilized in monitoring and control must be classified as Critical Cyber Assets, then the ability to provide remote support is not available to companies.

It is inherently not possible to implement all of the prescribed controls, i.e. CIP 006 physical controls, around workstations such as laptops when used from remote locations. The reliability of the Bulk Electric System will be eroded, rather than enhanced, if companies do not have the ability to remotely access the Critical Asset environment by utilizing laptop workstations with the cyber security controls prescribed in CIP 005.

Interpretation 2010-INT-05: Response to Request for an Interpretation of NERC Standard CIP-002-1 R3 for the Duke Energy Corporation

The following interpretation of NERC Standard CIP-002-1 Cyber Security — Critical Cyber Asset Identification was developed by a sub team of the Cyber Security Order 706 Standard Drafting Team.

Requirement Number and Text of Requirement

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a control center; or,
R3.3. The Cyber Asset is dial-up accessible.

Question 1

Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?

Response to Question 1

The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is ~~not intended to be~~ illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.

Question 2

What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the

Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.

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 essential to the operation of the Critical Asset. 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. Similarly, any Cyber Asset, when used to perform a function essential to the operation of the Critical Asset, becomes a Critical Cyber Asset.~~

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form
Interpretation 2010-INT-05
CIP-002-1 Requirement R3 for Duke Energy

Please **DO NOT** use this form to submit comments. Please use the electronic comment form located at the link below to submit comments on Interpretation 2010-INT-05 CIP-002-1 Requirement R3 for Duke Energy. The electronic comment form must be completed by **March 23, 2012.**

Additional information is available on the project page at: http://www.nerc.com/filez/standards/2010-INT-05_Interpretation_CIP-002-1_Duke.html

If you have questions please contact Steven Noess at steven.noess@nerc.net or by telephone at (404 446-9691).

Background Information

A 30-day formal comment period for this interpretation closed on October 8, 2010. Since that date, a project team from the CIP Interpretation Drafting Team has reviewed and responded to the comments received from that posting and made revisions to the interpretation encompassing Duke Energy's Request for Interpretation Questions 1 and 2. The project team revised the interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. (Available at: http://www.nerc.com/files/Guidelines_for_Interpretation_Drafting_Teams_Approved_April_2011.pdf)

Duke Energy asked two questions in their Request for Interpretation.

In response to Question 1, the Interpretation Drafting Team ("IDT") agreed with commenters that the interpretation to Question 1 was good. The IDT increased clarity by adding words to create the phrase, "is illustrative, not prescriptive." The examples given in Requirement 3 are illustrative and not prescriptive.

In response to Question 2, commenters strongly commented that the previously-posted interpretation was not satisfactory. With that result, the IDT researched the wording of the phrase and developed a new interpretation. "Essential" is not defined in the Glossary of Terms used in NERC Reliability Standards. However, the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." Either word may be used in place of "essential."

The IDT notes that the first posted draft of Version 5 of CIP-002 is addressing many of the issues raised in this Request for Interpretation.

Additionally, the IDT offers the following supplemental observation regarding the above interpretations. The language within CIP-002-1 Requirement 3 works hand-in-hand with the Standard's Purpose and Requirement 1. The Responsible Entity is responsible for using its judgment to identify Critical Cyber Assets that are essential, inherent, or necessary to the operation of the Critical Assets."

You do not have to answer all questions. Enter All Comments in Simple Text Format.
Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

Please review the request for an interpretation, the associated standard, and the draft interpretation and then answer the following questions.

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

Question #1:

☐ The request in Question 1 of the Request for Interpretation is asking for clarity on the **meaning** of a requirement.

☐ The request in Question 1 of the Request for Interpretation is asking for clarity on the **application** of a requirement.

Comments:

Question #2:

☐ The request in Question 2 of the Request for Interpretation is asking for clarity on the **meaning** of a requirement.

☐ The request in Question 2 of the Request for Interpretation is asking for clarity on the **application** of a requirement.

Comments:

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

Question #3:

☐ The interpretation for Question 1 of the Request for Interpretation **expands** the reach of the standard.

☐ The interpretation for Question 1 of the Request for Interpretation **does not expand** the reach of the standard.

Comments:

Question #4:

☐ The interpretation for Question 2 of the Request for Interpretation **expands** the reach of the standard.

☐ The interpretation for Question 2 of the Request for Interpretation **does not expand** the reach of the standard.

Comments:

Question #5:

Do you agree with the Interpretation Drafting Team's response to **Question 1** of the Request for Interpretation? If not, please explain specifically what you disagree with.

☐ Yes

☐ No

Comments:

Question #6:

Do you agree with the Interpretation Drafting Team's response to **Question 2** of the Request for Interpretation? If not, why not.

☐ Yes

☐ No

Comments:

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3

3. Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-26 Interpretation of CIP-004-x for WECC

Project 2010-INT-05 Interpretation of CIP-002-x for Duke

Two Ballot Windows (One Initial and One Successive)
Now Open Through 8 p.m. Eastern Friday, March 23, 2012

Now Available: Project 2009-26 | Project 2010-INT-05

The following ballot windows for two CIP interpretations are now open: 1) an initial ballot window for an interpretation of standard CIP-002-x — Critical Cyber Asset Identification, Requirements R3, and 2) a successive ballot window for an interpretation of standard CIP-004-x — Cyber Security — Personnel & Training, Requirements R2, R3, and R4, for WECC. Both ballot windows are open **until 8 p.m. EST on Friday, March 23, 2012.**

Instructions for Balloting on the Interpretations of CIP-002-x for Duke and CIP-004-x for WECC

Members of the ballot pools associated with each of these interpretations may log in and submit their votes for the interpretations by clicking here.

Special Instructions for Submitting Comments with a Ballot

Please note that each interpretation has a separate electronic comment form, and for each interpretation, comments submitted during the formal comment period and the ballot for the interpretation use the same electronic form. It is NOT necessary for ballot pool members to submit comments through the ballot application – **all comments should be submitted through the electronic comment form associated with the interpretation**.

Next Steps

The drafting team will consider all comments submitted to determine whether to make additional revisions to the interpretation.

Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP interpretations were developed by a different drafting team. The CIP Interpretation Drafting Team has reviewed all comments submitted in the previous postings of each interpretation, along with FERC orders issued since the previous posting,

and has revised the interpretations in response to comments and consistent with guidance adopted by the NERC Board of Trustees and Standards Committee.

Information about the CIP Interpretation Drafting team is available on the team's webpage, which contains links to each of the interpretations that the team is working on including the two being balloted now.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development and interpretation processes. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-26 Interpretation of CIP-004-x for WECC

Project 2010-INT-05 Interpretation of CIP-002-x for Duke

Two Ballot Pool Windows Now Open through 8 a.m. Eastern on March 8, 2012
Two Formal Comment Periods Open through Friday 8 p.m. March 23, 2012
Two Ballot Windows (One Initial and One Successive) Open March 14 – 23, 2012

Now Available Here:

Project 2010-INT-05 CIP-002-x Interpretation of CIP-002-x for Duke
Project 2009-26 Interpretation of CIP-004-x for WECC

The CIP Interpretation Drafting team has posted two CIP Interpretations for formal comment periods through 8 p.m. Eastern on Friday, March 23, 2012. Ballot pools are being formed for each interpretation through **8 a.m. Eastern on Thursday, March 8** (*please note that ballot pools close at 8 a.m. on the day they close*). Ballots of each interpretation will be conducted during the last ten days of the comment period, from Wednesday, March 14 through Friday, March 23, 2012, closing at 8 p.m. Eastern.

Instructions for Joining Ballot Pools

Separate ballot pools are being formed for each interpretation. Although a ballot pool was previously formed for Project 2009-26, the Standards Committee has authorized forming a new ballot pool to ensure that current Registered Ballot Body members have an opportunity to participate.

To join the ballot pools to be eligible to vote in the upcoming ballots of each interpretation, go to: Join Ballot Pool

During the pre-ballot windows, members of each ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the interpretations.

The list servers for each interpretation project are:

Project 2009-26 Interpretation of CIP-004-x for WECC: bp-2009-26_CIP-004-1_SB_in@nerc.com

Project 2010-INT-05 Interpretation of CIP-002-x for Duke Energy bp-2010-INT-05_CIP-002_in@nerc.com

Instructions for Commenting

A formal comment period is open for each interpretation through **8 p.m. Eastern on Friday, March 23, 2012**. Each interpretation has a separate comment form. Please use the links below to submit comments using the electronic comment form for each interpretation. Off-line, unofficial copies of the comment forms are posted on the project pages.

Project 2010-INT-05 Interpretation of CIP-002-x for Duke	Electronic comment form	Project page
Project 2009-26 Interpretation of CIP-004-x for WECC	Electronic comment form	Project page

If you experience any difficulties in using the electronic forms, please contact Monica Benson at monica.benson@nerc.net.

Next Steps

A successive ballot window will be open for the interpretation in Project 2009-26 Interpretation of CIP-004-x for WECC from Wednesday, March 14 through 8 p.m. Eastern on Friday, March 23, 2012.

An initial ballot window will be open for the interpretation in Project 2010-INT-05 Interpretation of CIP-002-x for Duke from Wednesday, March 14 through 8 p.m. Eastern on Friday, March 23, 2012.

Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP interpretations were developed by a different drafting team. The CIP Interpretation Drafting Team has reviewed all comments submitted in the previous postings of each interpretation, along with FERC orders issued since the previous posting, and has revised the interpretations in response to comments and consistent with guidance adopted by the NERC Board of Trustees and Standards Committee.

Additional information about each project is available on the individual project pages:

Project 2010-INT-05 Interpretation of CIP-002-x for Duke
Project 2009-26 Interpretation of CIP-004-x for WECC

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Project 2009-26 Interpretation of CIP-004-x for WECC
Project 2010-INT-05 Interpretation of CIP-002-x for Duke

Initial and Successive Ballot Results

Now Available 2009-26|2010-INT-05

Ballots of two CIP interpretations concluded Friday, March 23, 2012:

- An initial ballot of Project 2009-26 – Interpretation of CIP-004-x for WECC
- A successive ballot of Project 2010-INT-05 – Interpretation of CIP-002-x for Duke

Voting statistics for each ballot are listed below, and the Ballots Results page provides a link to the detailed results.

Standard	Quorum	Approval
Project 2009-26 Interpretation of CIP-004-x for WECC	Quorum: 88.55%	Approval: 79.61%
Project 2010-INT-05 Interpretation of CIP-002-x for Duke	Quorum: 89.63%	Approval: 94.71%

Next Steps

The CIP Interpretation Drafting Team (CIP IDT) will consider all comments submitted for each interpretation, and based on the comments, for each interpretation will determine whether to make additional revisions to the interpretation. If the drafting team determines that no substantive changes to the interpretation are required to address the comments, a recirculation ballot of the interpretation will be conducted. If the drafting team decides to make substantive revisions to either interpretation, the drafting team will submit the revised interpretation and consideration of the comments received for a quality review prior to posting for a parallel formal 30-day comment period and successive ballot.

Background

In May 2011 the Standards Committee appointed a standing CIP Interpretation Drafting team, and assigned these interpretations to that team.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

Ballot Results

Ballot Name:	Project 2010-INT-05 CIP-002-1 R3 for Duke Energy_in
Ballot Period:	3/14/2012 - 3/23/2012
Ballot Type:	Initial
Total # Votes:	294
Total Ballot Pool:	328
Quorum:	**89.63 % The Quorum has been reached**
Weighted Segment Vote:	94.71 %
Ballot Results:	**The drafting team is considering comments.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	82	1	66	0.985	1	0.015	10	5
2 - Segment 2.	10	0.7	7	0.7	0	0	2	1
3 - Segment 3.	77	1	66	0.985	1	0.015	3	7
4 - Segment 4.	23	1	20	1	0	0	1	2
5 - Segment 5.	75	1	55	0.982	1	0.018	7	12
6 - Segment 6.	44	1	35	0.972	1	0.028	4	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.7	6	0.6	1	0.1	0	1
9 - Segment 9.	2	0.1	1	0.1	0	0	0	1
10 - Segment 10.	7	0.6	4	0.4	2	0.2	0	1
Totals	**328**	**7.1**	**260**	**6.724**	**7**	**0.376**	**27**	**34**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain	View

1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	View
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Abstain	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer		
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Abstain	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Theresa Allard	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Abstain	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	View
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	

1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	View
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	View
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Ameren Services	Mark Peters	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Abstain	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	View
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Danny Lindsey	Affirmative	View
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	View
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	

3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen		
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	View
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Abstain	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	View
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	View
5	AEP Service Corp.	Brock Ondayko	Affirmative	View
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	View
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Colorado Springs Utilities	Jennifer Eckels	Abstain	

5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Abstain	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Affirmative	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	View
5	Essential Power, LLC	Patrick Brown	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh		
5	ICF International	Brent B Hebert	Abstain	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	View
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley		
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Abstain	
5	Puget Sound Energy, Inc.	Tom Flynn		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	View
5	Tacoma Power	Claire Lloyd	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Tri-State G & T Association, Inc.	Barry Ingold		
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	View
6	APS	RANDY A YOUNG	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	

6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Manitoba Hydro	Daniel Prowse	Affirmative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Powerex Corp.	Daniel W. O'Hearn		
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Abstain	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Affirmative	
8		Edward C Stein		
8	APX	Michael Johnson	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	View
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Name (20 Responses)
Organization (20 Responses)
Group Name (13 Responses)
Lead Contact (13 Responses)
Question 1 (32 Responses)
Question 1 Comments (33 Responses)
Question 2 (32 Responses)
Question 2 Comments (33 Responses)
Question 3 (32 Responses)
Question 3 Comments (33 Responses)
Question 4 (32 Responses)
Question 4 Comments (33 Responses)
Question 5 (33 Responses)
Question 5 Comments (33 Responses)
Question 6 (33 Responses)
Question 6 Comments (33 Responses)

Group
Tennessee Valley Authority
Brian Millard
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Jay Walker
NIPSCO
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes

Yes
Group
PacifiCorp
Sandra Shaffer
Yes
Yes
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Group
Northeast Power Coordinating Council
Guy Zito
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes

Yes
Individual
Randi Nyholm
Minnesota Power
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Thad Ness
American Electric Power
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Greg Rowland
Duke Energy
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the

standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
However, the interpretation could be improved by striking the parenthetical “(i.e., without which a Critical Asset cannot function as intended),” from the second paragraph. This parenthetical attempts to define the word “required”, which is not necessary for the interpretation.
Group
Southwest Power Pool Regional Entity
Emily Pennel
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation expands the reach of the standard.
As discussed in our comments to Question #5 below, the interpretation for Question 1 introduces a concept not present in the currently approved requirement.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
No
The response to Question 1 states that the examples of the types of Cyber Assets "should be considered." The language "should be considered" is not found in CIP-002/R3 and should not be inferred. While the SPP RE agrees that the list of example Cyber Assets enumerated in R3 is not all inclusive, the list does identify types of Cyber Assets that perform functions that are essential to the operation of the control center. As such, the examples are appropriately classified as Critical Cyber Assets *if* found in a control center that has been identified as a Critical Asset.
No
The response to Question 2 must be revised to specifically include the proviso that redundancy is NOT a consideration when determining if a Cyber Asset is "essential." Redundancy cannot be a consideration because, generally, vulnerability of the reduntant asset is the same as the primary asset’s vulnerability. To achieve security you have to consider both primary and redundant assets. The interpretation must also incorporate the provisions of CAN-0005 in such a way as to make CAN-0005 no longer necessary.
Individual
Michael Falvo
Independent Electricity System Operator
The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.

The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.
Since the language and intent of a reliability requirement is the ultimate arbiter of compliance, examples may be considered by some auditors to be more than just “information only”. Ingleside Cogeneration believes that the request is looking to ensure that a violation will not be assessed because an example is not addressed by a Responsible Entity in the process of identifying its Critical Cyber Assets.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
Question 2 revolves around the meaning of the term “essential” which determines if a Cyber Asset must be identified as a Critical Cyber Asset. This assessment becomes quite complex, especially in the case of mobile remote assets typically used in maintenance and trouble shooting. If CIP physical and electrical protections apply to such devices, some valuable capabilities will be lost. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Ingleside Cogeneration LP strongly agrees with the IDT’s interpretation that the examples given in R3 should be considered “illustrative, not prescriptive”. Our assessment shows two actions taken by NERC in regard to the requirement which support this clarification. First, the entire purpose of NERC’s security guideline for “Identifying Critical Cyber Assets” is to provide a means for Responsible Entities to establish which Cyber Assets should be critical. This is a 47 page document with multiple evaluations and complex procedural steps. Clearly a single sentence in a requirement cannot be considered to be exhaustive – or anything more than a suggestion. Second, the statement with the examples has been removed from CIP-002-4, presently pending FERC’s approval. It seems apparent to us that this action was taken because the examples only served to confuse Responsible Entities and auditors alike – and are more appropriately addressed in a guideline document.
Yes
We commend the Interpretation Drafting Team for developing a reading of the term “essential” based upon its commonly understood usage. We also agree that it is important to provide gradations which are close to the concept of essentiality, but does not meet the criticality litmus test. This allows the exclusion of Cyber Assets which “may be used, but not required” or are “merely valuable” to the inherent operation of the Critical Asset. It is left up to the Responsible Entity to make those assessments using an internal methodology that is comprehensive and defensible – and is consistent with the intent of CIP-002 as it is written today. We realize this flexibility may be limited in CIP version 5. However, those standards must still go through the vetting process; which will allow the industry to review, post comments, and vote upon any proposed changes.

Group
Bonneville Power Administration
Chris Higgins
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
BPA agrees that the examples in CIP-002 R3 are illustrative and not meant to be prescriptive.
Yes
BPA agrees that if a Cyber Asset is not required, merely “valuable to” the operation of a Critical Asset, it is not essential.
Individual
Kim Koster
MidAmerican Energy Company
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.
The request is asking for clarity on applying the requirement. The request is asking if laptops at remote locations have to comply with CIP-002 R3.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.
The request is seeking the definition for the term “essential.” Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms.
No
While we agree with the conclusion in the response to Question 1, we do not believe this interpretation is needed at this time. The response does not provide any new information.
No
MidAmerican Energy does not believe this interpretation is needed at this time. The request is seeking the definition for the term “essential.” Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms. The interpretation provides no new useful information and creates more confusion by introducing the new term “inherent to.”
Group
ISO/RTO Council Standards Review Committee
Christine Hasha
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.

The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Group
Dominion
Connie Lowe
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Kirit Shah
Ameren
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes

Yes
Individual
Jonathan Appelbaum
United Illuminating Company
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Thomas Johnson
Salt River Project
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
David Thorne
Pepco Holdings Inc
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the

standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Andrew Gallo
City of Austin dba Austin Energy
The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Group
FirstEnergy
Sam Ciccone
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Since there are no question for general comments, we offer them in this last question. Just as a reminder, this Interpretation, once approve, will also need to be added to the pending CIP-002-4 standard which is currently before FERC for approval. It would seem that the Interpretation, if approved, could be added to the Version 4 standard as an errata change.

Group
Southern Company
Shane Eaker
The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.
The question asks if the examples provided are prescribed to be CCAs or types of equipment that could be assessed as possible CCAs.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The question asks for clarification about the meaning of the word “essential.”
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The clarification that the examples are illustrative is helpful in understanding the requirement, but does not expand the reach of the requirement.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
The response to question 2 does not expand the reach of the standard but provides clarity around which cyber assets are essential vs. assets that are valuable but not essential.
Yes
Yes
Individual
Patrick Brown
Essential Power, LLC
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Group
Kansas City Power & light
Scott Harris
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.

The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
IDT clearly defines “essential” in its response. More importantly it states a “valuable” asset is not necessarily “essential” to the operatation of a Critical Asset, thereby, indirectly addressing Duke’s concern with physical controls around workstations such as laptops when used from remote locations.
Individual
Anthony Jablonski
ReliabilityFirst
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 could be construed as restricting the reach of the standard.
Yes
No
The Interpretation’s “Response to Question 2” may render CIP-002-3 through CIP-009-3 non-functional. The statement, “A Cyber Asset that ‘may’ be used, but is not ‘required’ (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not ‘essential to the operation of the Critical Asset’ for purposes of Requirement R3” transforms CIP-002-3 R3 into a single point of failure analysis. Cyber systems used in the operation of the BES are designed so there is no single point of failure. Therefore, there would be no Critical Cyber Assets in the meaning stated by the “Response to Question 2.” The Interpretation must be revised to make clear that any Cyber Asset, even if replicated locally or remotely, that, if damaged, lost or compromised, can have a negative impact on the reliable operation of the associated Critical Asset must be identified as a Critical Cyber Asset.
Individual
Ron Donahey
Tampa Electric Company
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.

The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Tampa Electric agrees with the Interpretations Drafting Team response to Question 1
Yes
Tampa Electric agrees with the Interpretations Drafting Team response to Question 2. We strongly support the concept that essential to the operation of the Critical Asset means that it is necessary for the operation of that Critical Asset.
Group
MISO Standards Collaborators
Marie Knox
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request seeks clarification of whether the phrase at issue is illustrative or prescriptive. 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 request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in CIP-002. 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 for Question 1 of the Request for Interpretation does not expand the reach of the standard.
MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.
MISO submits that, by clarifying that a Critical Cyber Asset ("CCA") must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Yes
MISO agrees with the Interpretation as to Question 1.
Yes
MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that “essential,” as used in Requirement R3, is synonymous with “inherent”, “necessary” and “required”. MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity’s determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.
Individual
Christina Bigelow
Midwest ISO
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request seeks clarification of whether the phrase at issue is illustrative or prescriptive. 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 request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in

CIP-002. 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 for Question 1 of the Request for Interpretation does not expand the reach of the standard.
MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
MISO submits that, by clarifying that a Critical Cyber Asset ("CCA") must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Yes
MISO agrees with the Interpretation as to Question 1.
Yes
MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that “essential,” as used in Requirement R3, is synonymous with “inherent”, “necessary” and “required”. MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity’s determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.
Group
ACES Power Marketing Standards Collaborators
Jason Marshall
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
While we agree with the drafting team, we recommend rewording “(i.e. without which a Critical Asset cannot function as intended)” to “(i.e. the Critical Asset cannot function without the Cyber Asset)”. While the wording is technically correct, it is difficult to read and can be confusing.
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.

The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes
Individual
Joe Doetzl
CRSI
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
No
The definition provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. The interpretation does not provide additional clarity than what is provided in the existing guideline.
Individual
Darryl Curtis
Oncor Electric Delivery Company
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes

Individual
DANA SHOWALTER
E.ON CLIMATE & RENEWABLES
The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.
The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.
The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.
Yes
Yes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation 2010-INT-05
CIP-002-1 Requirement R3 for Duke Energy

The CIP-002-1 Requirement R3 Drafting Team thanks all commenters who submitted comments on Interpretation 2010-INT-05 CIP-002-1 Requirement R3 for Duke Energy. These standards were posted for a 45-day public comment period from February 8, 2012 through March 23, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 33 sets of comments, including comments from approximately 91 different people from approximately 58 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/2010-INT-05_Interpretation_CIP-002-1_Duke.html

Summary:

The IDT carefully reviewed all comments in response to the posting for parallel formal comment period and ballot that ended March 23, 2012. In the draft interpretation the IDT sought to clarify for Duke Energy that the examples given in CIP-002-x, Requirement R3 are illustrative, not prescriptive. The IDT also sought to clarify the meaning of the phrase "essential to the operation of the Critical Asset" as requested by Duke Energy, because the requirement specifies that "the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset." The IDT clarifies that a Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. The IDT made one clarifying change to reword a parenthetical phrase, and the IDT made no further changes to the interpretation. Many commenters agreed with the interpretation and several comments provided additional justification in support of the interpretation, and the IDT explains its rationale in response to several minority concerns below. The interpretation will be posted for a recirculation ballot.

- There were a few commenters that believe the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that in this case, it appears to be a question of semantics, where the IDT and industry both believe, overall, that the request is asking for clarity on the meaning of a requirement.
- Some commenters suggest that the interpretation could be construed as restricting the reach of the standard or that the interpretation is unnecessary or does not add new information, but the IDT disagrees. The IDT acknowledges that the interpretation may be construed to restrict many

parties or individuals' prior, different understanding or organizational interpretation of the reach of the standard. Furthermore, the interpretation is necessary because it provides clarity for all entities.

- A commenter disagreed with the interpretation by noting that the response to Question 1 states that the types of Cyber Assets in the example "should be considered," and the language "should be considered" is not found in CIP-002-3, Requirement R3 and should not be inferred. The IDT explains that the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, which requires some "consideration" within the context of the requirement.
- One commenter suggested that Version 4's language may have a similar issue. The IDT notes that an interpretation applies only so long as the relevant language in a standard is in effect, and it agrees that this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists.
- One commenter agreed with the Interpretation as to Question 2, but requested that the IDT clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". The commenter also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a Critical Asset. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, the IDT does agree that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct.
- Two commenters commented on the parenthetical clause in the original interpretation, suggesting that it was confusing upon first reading the language or that it seems to define "required." One commenter suggested rewording the clause, and one commenter suggested removing the clause as unnecessary. The IDT agrees, and it re-worded the clause from "(i.e. without which a Critical Asset cannot function as intended)" to, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)." This is a clarifying change, and it is not substantive.
- One commenter suggested that the IDT incorporate the provisions of NERC's CAN-0005 so that the CAN may be retired. The IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005.
- Other commenters were concerned that the interpretation does not explicitly state that redundancy is not a consideration for identifying Cyber Assets that are "essential." The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.

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

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

Index to Questions, Comments, and Responses

The Industry Segments are:

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

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

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

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

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

2.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

No additional members listed.

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

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

4.	Group	Christine Hasha	ISO/RTO Council Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Gary DeShazo	CAISO	WECC	2

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

3.	Steve Myers	ERCOT	ERCOT	2
4.	Ben Li	IESO	NPCC	2
5.	Kathleen Goodman	ISONE	NPCC	2
6.	Marie Knox	MISO	RFC	2
7.	Donald Weaver	NBSO	NPCC	2
8.	Greg Campoli	NYISO	NPCC	2
9.	Al DiCaprio	PJM	RFC	2
10.	Charles Yeung	SPP	SPP	2

5.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	5
3.	Louis Slade		RFC	5
4.	Michael Gildea		MRO	5

6.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hohlbaugh	FE	RFC	

7.	Group	Scott Harris	Kansas City Power & light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dean Larson	Kansas City Power & Light	SPP	1, 3, 5, 6
2.	Michael Gammon	Kansas City Power & Light	SPP	1, 3, 5, 6

8.	Group	Marie Knox	MISO Standards Collaborators								X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Cyrulewski	JDRJC Associates, LLC	RFC	8

9.	Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
2.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
3.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
4. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
5. Bob Solomon		Hoosier Energy	RFC 1										
10.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Mauricio Lopez	IID	WECC	1, 3, 4, 5, 6									
2.	Israel Gonzalez	IID	WECC	1, 3, 4, 5, 6									
3.	Peter Nguyen	IID	WECC	1, 3, 4, 5, 6									
11.	Individual	Brian Millard	Tennessee Valley Authority	X		X		X	X				
12.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
13.	Individual	Shane Eaker	Southern Company	X		X		X	X				
14.	Individual	Jay Walker	NIPSCO	X		X		X	X				
15.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
16.	Individual	Randi Nyholm	Minnesota Power	X		X		X	X				
17.	Individual	Thad Ness	American Electric Power	X		X		X	X				
18.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
19.	Individual	Michael Falvo	Independent Electricity System Operator		X								
20.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
21.	Individual	Kim Koster	MidAmerican Energy Company	X		X		X	X				
22.	Individual	Kirit Shah	Ameren	X		X		X	X				
23.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
24.	Individual	Thomas Johnson	Salt River Project	X		X		X	X				
25.	Individual	David Thorne	Pepco Holdings Inc	X		X							
26.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
27.	Individual	Patrick Brown	Essential Power, LLC	X				X					
28.	Individual	Anthony Jablonski	ReliabilityFirst										X
29.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
30.	Individual	Christina Bigelow	Midwest ISO		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
31.	Individual	Joe Doetzl	CRSI										
32.	Individual	Darryl Curtis	Oncor Electric Delivery Company	X									
33.	Individual	DANA SHOWALTER	E.ON CLIMATE & RENEWABLES					X					

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

☐ **The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.**

☐ **The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.**

Summary Consideration:

Most commenters agreed that question 1 of the request for interpretation is asking for clarity on the meaning of a requirement, and the IDT agrees. There were a few commenters that believe question 1 of the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that in this case, it appears to be a question of semantics, where the IDT and industry both believe, overall, that the request is asking for clarity on the meaning of a requirement.

Organization	Yes or No	Question 1 Comment
Southern Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	The question asks if the examples provided are prescribed to be CCAs or types of equipment that could be assessed as possible CCAs.
Response: Thanks for your comment and supporting rationale. This appears to be a question of semantics, where the IDT and industry majority believe, overall, that the request asks for clarity on the meaning of a requirement.		
Ingleside Cogeneration LP	The request in Question 1 of the Request for Interpretation is asking for clarity on the	Since the language and intent of a reliability requirement is the ultimate arbiter of compliance, examples may be considered by some auditors to be more than just "information only". Ingleside Cogeneration believes that the

Organization	Yes or No	Question 1 Comment
	application of a requirement.	request is looking to ensure that a violation will not be assessed because an example is not addressed by a Responsible Entity in the process of identifying its Critical Cyber Assets.
Response: Thanks for your comment and supporting rationale. This appears to be a question of semantics, where the IDT and industry majority believe, overall, that the request asks for clarity on the meaning of a requirement.		
Independent Electricity System Operator	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	
City of Austin dba Austin Energy	The request in Question 1 of the Request for Interpretation is asking for clarity on the application of a requirement.	
MISO Standards Collaborators	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of whether the phrase at issue is illustrative or prescriptive. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thank you for your comment, which agrees with this IDT's position.		
Midwest ISO	The request in Question 1	The request seeks clarification of whether the phrase at issue

Organization	Yes or No	Question 1 Comment
	of the Request for Interpretation is asking for clarity on the meaning of a requirement.	is illustrative or prescriptive. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment and supporting rationale, which agrees with this IDT's position on the question.		
Northeast Power Coordinating Council	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Southwest Power Pool Regional Entity	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Bonneville Power Administration	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ISO/RTO Council Standards Review Committee	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Dominion	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
FirstEnergy	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Kansas City Power & light	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Imperial Irrigation District (IID)	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Tennessee Valley Authority	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
NIPSCO	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Transmission Company, LLC	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Minnesota Power	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Electric Power	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Duke Energy	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
MidAmerican Energy Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Ameren	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
United Illuminating Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Salt River Project	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Pepco Holdings Inc	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Essential Power, LLC	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ReliabilityFirst	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tampa Electric Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
CRSI	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 1 Comment
Oncor Electric Delivery Company	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
E.ON CLIMATE & RENEWABLES	The request in Question 1 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

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

☐ **The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.**

☐ **The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.**

Summary Consideration:

Much like question 1, most commenters agree with the IDT that question 2 of the request for interpretation asks for clarity on the meaning of a requirement. Some commenters believe that the request asks for clarity on the application of a requirement, noting that the request asks if laptops at remote locations have to comply with CIP-002, Requirement R3. The IDT agrees that there may be an application component, but on balance, the request is asking for clarity. The IDT believes that the laptops illustration was provided as an example of why further clarity is needed in order to help the industry understand this requirement. One commenter asked whether the IDT believes the interpretation expands the scope of the requirement. The IDT does not.

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.	The request is asking for clarity on applying the requirement. The request is asking if laptops at remote locations have to comply with CIP-002 R3.
Response: Thanks for your comment and rationale, however the IDT believes that the laptops illustration was provided as an example of why further clarity is needed in order to help the industry understand this requirement.		
Salt River Project	The request in Question 2 of the Request for Interpretation is asking for	

Organization	Yes or No	Question 2 Comment
	clarity on the application of a requirement.	
City of Austin dba Austin Energy	The request in Question 2 of the Request for Interpretation is asking for clarity on the application of a requirement.	
MISO Standards Collaborators	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in CIP-002. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Southern Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The question asks for clarification about the meaning of the word "essential."
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Ingleside Cogeneration LP	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	Question 2 revolves around the meaning of the term "essential" which determines if a Cyber Asset must be identified as a Critical Cyber Asset. This assessment becomes quite complex, especially in the case of mobile remote assets typically used in maintenance and trouble shooting. If CIP physical and electrical protections apply to such devices, some valuable capabilities will be lost. The NERC

Organization	Yes or No	Question 2 Comment
		Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?
Response: Thanks for your comment and provided rationale. The IDT views the remote laptops discussion as illustrative of why clarity needs to be provided surrounding the exact nature of this requirement. By rendering further clarity and then responding back to how it may affect that particular illustration, we have not substantively expanded the scope of the requirement.		
Midwest ISO	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	The request seeks clarification of the meaning of "essential to the operation of the Critical Asset" in CIP-002. As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Southwest Power Pool Regional Entity	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Bonneville Power	The request in Question 2 of	

Organization	Yes or No	Question 2 Comment
Administration	the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ISO/RTO Council Standards Review Committee	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Dominion	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
FirstEnergy	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Kansas City Power & light	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ACES Power Marketing Standards Collaborators	The request in Question 2 of the Request for	

Organization	Yes or No	Question 2 Comment
	Interpretation is asking for clarity on the meaning of a requirement.	
Imperial Irrigation District (IID)	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tennessee Valley Authority	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
NIPSCO	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
American Transmission Company, LLC	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Minnesota Power	The request in Question 2 of the Request for Interpretation is asking for	

Organization	Yes or No	Question 2 Comment
	clarity on the meaning of a requirement.	
American Electric Power	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Duke Energy	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Independent Electricity System Operator	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Ameren	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
United Illuminating Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a	

Organization	Yes or No	Question 2 Comment
	requirement.	
Pepco Holdings Inc	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Essential Power, LLC	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
ReliabilityFirst	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
Tampa Electric Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
CRSI	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

Organization	Yes or No	Question 2 Comment
Oncor Electric Delivery Company	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	
E.ON CLIMATE & RENEWABLES	The request in Question 2 of the Request for Interpretation is asking for clarity on the meaning of a requirement.	

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

☐ **The interpretation for Question 1 of the Request for Interpretation expands the reach of the standard.**

☐ **The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.**

Summary Consideration:

Many commenters agreed with the IDT's interpretation relating to Question 1 of the Request for Interpretation, noting agreement that the interpretation clarifies that the list of examples is illustrative, not prescriptive. Other commenters noted that the interpretation provides clarity and does not expand the reach of the standard. One commenter suggested that the interpretation introduces a concept not in the requirement, and references its explanation in comments provided in support of question 5 of this comment form. The IDT responds to this in response to consideration of comments for question 5.

Organization	Yes or No	Question 3 Comment
MISO Standards Collaborators	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Southern Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	The clarification that the examples are illustrative is helpful in understanding the requirement, but does not expand the reach of the requirement.

Organization	Yes or No	Question 3 Comment
Response: Thanks for your supporting comment.		
Midwest ISO	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that the list of examples at control centers and backup control centers in Requirement R3 is illustrative and not presriptive, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Bonneville Power Administration	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ISO/RTO Council Standards Review Committee	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Dominion	The interpretation for Question 1 of the Request for Interpretation does	

Organization	Yes or No	Question 3 Comment
	not expand the reach of the standard.	
FirstEnergy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Kansas City Power & light	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ACES Power Marketing Standards Collaborators	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Imperial Irrigation District (IID)	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Tennessee Valley Authority	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of	

Organization	Yes or No	Question 3 Comment
	the standard.	
NIPSCO	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Minnesota Power	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Duke Energy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Independent Electricity System Operator	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Ingleside Cogeneration LP	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
MidAmerican Energy Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Ameren	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
United Illuminating Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Salt River Project	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Pepco Holdings Inc	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
City of Austin dba Austin Energy	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Essential Power, LLC	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
ReliabilityFirst	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 3 Comment
Tampa Electric Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
CRSI	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
E.ON CLIMATE & RENEWABLES	The interpretation for Question 1 of the Request for Interpretation does not expand the reach of the standard.	
Southwest Power Pool Regional Entity	The interpretation for Question 1 of the Request for Interpretation expands the reach of the standard.	As discussed in our comments to Question #5 below, the interpretation for Question 1 introduces a concept not present in the currently approved requirement.

Organization	Yes or No	Question 3 Comment
Response: See IDT's response to Southwest Power Pool Regional Entity's Question #5 comments below.		

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

☐ **The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.**
☐ **The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.**

Summary Consideration:

Most commenters agree that the interpretation for question 2 of the Request for Interpretation does not expand the reach of the standard, but, rather, provides clarity around which Cyber Assets are essential compared to those that are merely valuable but not essential.

Some commenters suggest that the interpretation could be construed as restricting the reach of the standard, but the IDT disagrees. The IDT acknowledges that the interpretation may be construed to restrict many parties or individuals' prior, different understanding or organizational interpretation of the reach of the standard.

One commenter suggested the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term, either in an interpretation or in the NERC Glossary of Terms. The IDT observed that several definitions exist for this word, but it disagrees that the interpretation is unnecessary. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity relating to the Requirement itself.

Organization	Yes or No	Question 4 Comment
Southern Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	The response to question 2 does not expand the reach of the standard but provides clarity around which cyber assets are essential vs. assets that are valuable but not essential.

Organization	Yes or No	Question 4 Comment
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
ReliabilityFirst	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	The interpretation for Question 2 could be construed as restricting the reach of the standard.
Response: Thanks for your comment providing rationale. While the IDT disagrees that this interpretation restricts the original reach of this requirement, we do agree that it may be construed to restrict other parties' prior understanding or organizational interpretation of the reach of this requirement.		
Midwest ISO	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	MISO submits that, by clarifying that a Critical Cyber Asset ("CCA") must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Northeast Power Coordinating Council	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Southwest Power Pool Regional Entity	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the	

Organization	Yes or No	Question 4 Comment
	standard.	
Bonneville Power Administration	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
ISO/RTO Council Standards Review Committee	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Dominion	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
FirstEnergy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Kansas City Power & light	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
ACES Power Marketing Standards Collaborators	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Imperial Irrigation District (IID)	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Tennessee Valley Authority	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
NIPSCO	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
American Transmission Company, LLC	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Minnesota Power	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
American Electric Power	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Duke Energy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Independent Electricity System Operator	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Ingleside Cogeneration LP	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Ameren	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
United Illuminating Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Salt River Project	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Pepco Holdings Inc	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
City of Austin dba Austin Energy	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	

Organization	Yes or No	Question 4 Comment
Essential Power, LLC	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Tampa Electric Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
CRSI	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
Oncor Electric Delivery Company	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
E.ON CLIMATE & RENEWABLES	The interpretation for Question 2 of the Request for Interpretation does not expand the reach of the standard.	
MISO Standards	The interpretation for	MISO submits that, by clarifying that a Critical Cyber Asset ("CCA")

Organization	Yes or No	Question 4 Comment
Collaborators	Question 2 of the Request for Interpretation expands the reach of the standard.	must be required by a Critical Asset ("CA") such that the CA cannot function as intended without the CCA, the Interpretation does not expand the reach or scope of the standard.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MidAmerican Energy Company	The interpretation for Question 2 of the Request for Interpretation expands the reach of the standard.	The request is seeking the definition for the term "essential." Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms.
Response: Thanks for your comment and provided rationale. The IDT observed that several definitions exist for this word. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity to the Requirement itself.		

5. Do you agree with the Interpretation Drafting Team's response to *Question 1* of the Request for Interpretation? If not, please explain specifically what you disagree with.

Summary Consideration:

Most commenters agreed with the IDT's interpretation to question 1 of the Request for Interpretation. One commenter noted that guidance documents are often very long, and that one string of examples in the requirement could not be exhaustive. Furthermore, that commenter noted that the statement with the examples has been removed from CIP-002-4, presently pending FERC's approval, and that it seems apparent to that commenter that this action was taken because the examples only served to confuse Responsible Entities and auditors alike - and are more appropriately addressed in a guideline document. Both of those comments and rationales support the IDT's view that the list is illustrative, not prescriptive.

A commenter disagreed with the interpretation by noting that the response to Question 1 states that the types of Cyber Assets in the example "should be considered," and the language "should be considered" is not found in CIP-002-3, Requirement R3 and should not be inferred. The commenter agrees that the list of example Cyber Assets enumerated in Requirement R3 is not all inclusive, but notes that the list does identify types of Cyber Assets that perform functions that are essential to the operation of the control center. As such, the commenters suggests that examples are appropriately classified as Critical Cyber Assets *if* found in a control center that has been identified as a Critical Asset. In response, the IDT noted that the interpretation's response to Question 1 clarifies that the examples are illustrative. Thus, since it is not a prescriptive list, those examples "should be considered" to determine whether they meet the requirement's language. Since the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, some consideration is necessary within the context of the requirement.

One commenter agreed with the interpretation, but does not believe that the interpretation is necessary or adds new information. In response, the IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.

Organization	Yes or No	Question 5 Comment
Alberta Electric System Operator	Abstain	The AESO agrees with the interpretation of CIP-002, however we are casting an abstain vote as this standard is not applicable in Alberta at this time.

Organization	Yes or No	Question 5 Comment
Response: Thanks for providing the IDT with your rationale.		
Bonneville Power Administration	Affirmative	please refer to BPA's submitted comments
Brazos Electric Power Cooperative, Inc.	Affirmative	See comments submitted by ACES Power Marketing.
Consolidated Edison Co. of New York	Affirmative	See NPCC region-wide group comment form
FirstEnergy Corp.	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Southern Company Services, Inc.	Affirmative	See comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
California ISO	Affirmative	Comments provided jointly with the ISO/RTO Standards Review Committee
Electric Reliability Council of Texas, Inc.	Affirmative	ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee
AEP	Affirmative	Response is being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Alabama Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
FirstEnergy Energy Delivery	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Georgia Power Company	Affirmative	See electronic comments submitted by John Horishny.

Organization	Yes or No	Question 5 Comment
Gulf Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Mississippi Power	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form
Ohio Edison Company	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Wisconsin Energy Corp.	Affirmative	Comments are requested to be submitted using the separate electronic comment form rather than with the vote. I strongly support this interpretation and do not have any specific comments to submit with this vote.
AEP Service Corp.	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Bonneville Power Administration	Affirmative	Please see BPA comments submitted via the electronic comment form.
Brazos Electric Power Cooperative, Inc.	Affirmative	Please see comments filed by ACES Power Marketing.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Occidental Chemical	Affirmative	See comments by submitted by Ingleside Cogeneration LP
Southern Company Generation	Affirmative	Please see Southern Company comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
AEP Marketing	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of

Organization	Yes or No	Question 5 Comment
		American Electric Power.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period
Northern Indiana Public Service Co.	Affirmative	see NIPSCO comments submitted
Southern Company Generation and Energy Marketing	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
Bonneville Power Administration	Yes	BPA agrees that the examples in CIP-002 R3 are illustrative and not meant to be prescriptive.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MISO Standards Collaborators	Yes	MISO agrees with the Interpretation as to Question 1.
Response: The IDT recognizes this affirmation as limited only to Question 1		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP strongly agrees with the IDT's interpretation that the examples given in R3 should be considered "illustrative, not prescriptive". Our assessment shows two actions taken by NERC in regard to the requirement which support this clarification. First, the entire purpose of NERC's security guideline for "Identifying Critical Cyber Assets" is to provide a means for Responsible Entities to establish which Cyber Assets should be critical. This is a 47 page document with multiple evaluations and complex procedural steps. Clearly a single sentence in a requirement cannot be considered to be exhaustive - or anything more than a suggestion. Second, the statement with the examples has been removed from CIP-

Organization	Yes or No	Question 5 Comment
		002-4, presently pending FERC's approval. It seems apparent to us that this action was taken because the examples only served to confuse Responsible Entities and auditors alike - and are more appropriately addressed in a guideline document.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
Tampa Electric Company	Yes	Tampa Electric agrees with the Interpretations Drafting Team response to Question 1
Response: The IDT recognizes this affirmation as limited only to Question 1		
Midwest ISO	Yes	MISO agrees with the Interpretation as to Question 1.
Response: The IDT recognizes this affirmation as limited only to Question 1		
Northeast Power Coordinating Council	Yes	
ISO/RTO Council Standards Review Committee	Yes	
Dominion	Yes	
FirstEnergy	Yes	
Kansas City Power & light	Yes	
ACES Power Marketing Standards Collaborators	Yes	
Imperial Irrigation District (IID)	Yes	
Tennessee Valley Authority	Yes	

Organization	Yes or No	Question 5 Comment
PacifiCorp	Yes	
Southern Company	Yes	
NIPSCO	Yes	
American Transmission Company, LLC	Yes	
Minnesota Power	Yes	
American Electric Power	Yes	
Duke Energy	Yes	
Independent Electricity System Operator	Yes	
Ameren	Yes	
United Illuminating Company	Yes	
Salt River Project	Yes	
Pepco Holdings Inc	Yes	
City of Austin dba Austin Energy	Yes	
Essential Power, LLC	Yes	

Organization	Yes or No	Question 5 Comment
ReliabilityFirst	Yes	
CRSI	Yes	
Oncor Electric Delivery Company	Yes	
E.ON CLIMATE & RENEWABLES	Yes	
MidAmerican Energy Co.	Negative	See MidAmerican comments
Southwest Power Pool Regional Entity	No	The response to Question 1 states that the examples of the types of Cyber Assets "should be considered." The language "should be considered" is not found in CIP-002/R3 and should not be inferred. While the SPP RE agrees that the list of example Cyber Assets enumerated in R3 is not all inclusive, the list does identify types of Cyber Assets that perform functions that are essential to the operation of the control center. As such, the examples are appropriately classified as Critical Cyber Assets *if* found in a control center that has been identified as a Critical Asset.
Response: Thanks for providing your rationale for response. The interpretation's response to Question 1 clarifies that the examples are illustrative. Thus, since it is not a prescriptive list, those examples "should be considered" to determine whether they meet the requirement's language. Since the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, some consideration is necessary within the context of the requirement.		
MidAmerican Energy Company	No	While we agree with the conclusion in the response to Question 1, we do not believe this interpretation is needed at this time. The response does not provide any new information.
Response: The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation		

Organization	Yes or No	Question 5 Comment
provides necessary clarity for all entities.		

6. Do you agree with the Interpretation Drafting Team's response to Question 2 of the Request for Interpretation? If not, why not.

Summary Consideration:

Most commenters agreed with the IDT's interpretation with respect to question 2 of the request for interpretation, and they agreed with the IDT's rationale that if a Cyber Asset is not required, but is merely "valuable to" the operation of a Critical Asset, it is not essential.

One commenter suggested that Version 4's language may have a similar issue. The IDT notes that an interpretation applies only so long as the relevant language in a standard is in effect, and it agrees that this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists.

One commenter agreed with the Interpretation as to Question 2, but requested that the IDT clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". The commenter also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a Critical Asset and therefore a Critical Cyber Asset pursuant to the clarification provided by the Interpretation. The commenter states that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct. As the majority of industry agreed with this balloted draft's current explanation of essential, the IDT did not incorporate the proposed change. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, the IDT does agree that a Registered Entity's determination of whether a Cyber Asset is required by a Critical Asset should be rebuttably presumed to be correct.

Two commenters commented on the parenthetical clause in the original interpretation, suggesting that it was confusing upon first reading the language or that it seems to define "required." One commenter suggested rewording the clause, and one commenter suggested removing the clause as unnecessary. The IDT agrees, and it re-worded the clause from "(i.e. without which a Critical Asset cannot function as intended)" to, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)." This is a clarifying change, and it is not substantive.

One commenter suggested that the IDT incorporate the provisions of NERC's CAN-0005 so that the CAN may be retired. While the IDT understands this interpretation's rationale to be in keeping with CAN-0005 and possibly forthcoming CIP versions, the IDT is bound by the Guidelines for Interpretation Drafting teams to interpret the words on the page of any standard being interpreted. The IDT believes that incorporating the submitted suggestions would expand the scope of the requirement in question. Furthermore, the IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005.

Other commenters were concerned that the interpretation does not explicitly state that redundancy is not a consideration for identifying Cyber Assets that are "essential." The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.

One commenter suggested the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms. The IDT observed that several definitions exist for this word, but it disagrees that the interpretation is unnecessary. The IDT clarified the meaning as it applies within the four corners of this particular standard's wording and scope, and it added context-sensitive clarity to the Requirement itself.

One commenter believed that the clarification provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, and that the interpretation does not provide additional clarity than what is provided in the existing guideline. The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.

Organization	Yes or No	Question 5 Comment
Alberta Electric System Operator	Abstain	The AESO agrees with the interpretation of CIP-002, however we are casting an abstain vote as this standard is not applicable in Alberta at this time.
Response: Thanks for providing the IDT with your rationale.		
Bonneville Power	Affirmative	please refer to BPA's submitted comments

Organization	Yes or No	Question 5 Comment
Administration		
Brazos Electric Power Cooperative, Inc.	Affirmative	See comments submitted by ACES Power Marketing.
Consolidated Edison Co. of New York	Affirmative	See NPCC region-wide group comment form
FirstEnergy Corp.	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Southern Company Services, Inc.	Affirmative	See comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
California ISO	Affirmative	Comments provided jointly with the ISO/RTO Standards Review Committee
Electric Reliability Council of Texas, Inc.	Affirmative	ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee
AEP	Affirmative	Response is being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Alabama Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.
FirstEnergy Energy Delivery	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Georgia Power Company	Affirmative	See electronic comments submitted by John Horishny.
Gulf Power Company	Affirmative	See comments submitted in the electronic comments form by John Horishny.

Organization	Yes or No	Question 5 Comment
Mississippi Power	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form
Ohio Edison Company	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Wisconsin Energy Corp.	Affirmative	Comments are requested to be submitted using the separate electronic comment form rather than with the vote. I strongly support this interpretation and do not have any specific comments to submit with this vote.
AEP Service Corp.	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.
Bonneville Power Administration	Affirmative	Please see BPA comments submitted via the electronic comment form.
Brazos Electric Power Cooperative, Inc.	Affirmative	Please see comments filed by ACES Power Marketing.
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period.
Occidental Chemical	Affirmative	See comments by submitted by Ingleside Cogeneration LP
Southern Company Generation	Affirmative	Please see Southern Company comments submitted by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
AEP Marketing	Affirmative	Comments are being submitted via electronic form by Thad Ness on behalf of American Electric Power.

Organization	Yes or No	Question 5 Comment
FirstEnergy Solutions	Affirmative	Please see FirstEnergy's comments submitted through the formal comment period
Northern Indiana Public Service Co.	Affirmative	see NIPSCO comments submitted
Southern Company Generation and Energy Marketing	Affirmative	See comments submitted in the electronic comments form by John Horishny.
Tennessee Valley Authority	Affirmative	Please see TVA's comments submitted through the electronic comment form.
Bonneville Power Administration	Yes	BPA agrees that if a Cyber Asset is not required, merely "valuable to" the operation of a Critical Asset, it is not essential.
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
FirstEnergy	Yes	Since there are no question for general comments, we offer them in this last question.Just as a reminder, this Interpretation, once approve, will also need to be added to the pending CIP-002-4 standard which is currently before FERC for approval. It would seem that the Interpretation, if approved, could be added to the Version 4 standard as an errata change.
Response: Thanks for your additional comment. As an interpretation applies only so long as the relevant language in a standard is in effect, we agree this interpretation might be applicable for clarifying CIP Version 4, provided the same lack of clarity persists, which First Energy apparently believes to be the case.		
Kansas City Power & light	Yes	IDT clearly defines "essential" in its response. More importantly it states a "valuable" asset is not necessarily "essential" to the operatation of a Critical Asset, thereby, indirectly addressing Duke's concern with physical controls around workstations such as laptops when used from remote locations.

Organization	Yes or No	Question 5 Comment
Response: Thanks for your comment providing rationale that reinforces the IDT's position on this question.		
MISO Standards Collaborators	Yes	MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity's determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.
Response: Thanks for your provided rationale. As the majority of industry agreed with this balloted draft's current explanation of essential, we have not incorporated the proposed change. Much like the list of examples is illustrative, the IDT agrees with most commenters that the interpretation provides clarity, and it is not necessary at this time to list further synonyms for "essential." Further, we agree with the MISO commenting body's final conclusion.		
ACES Power Marketing Standards Collaborators	Yes	While we agree with the drafting team, we recommend rewording "(i.e. without which a Critical Asset cannot function as intended)" to "(i.e. the Critical Asset cannot function without the Cyber Asset)". While the wording is technically correct, it is difficult to read and can be confusing.
Response: Thanks for your suggestion, which has been considered within the next draft. The IDT reworded the clause, but not the meaning or substance, so that it now reads, "(i.e., a Critical Asset cannot function as intended without the Cyber Asset)"		
Duke Energy	Yes	However, the interpretation could be improved by striking the parenthetical "(i.e., without which a Critical Asset cannot function as intended)," from the second paragraph. This parenthetical attempts to define the word "required", which is not necessary for the interpretation.
Response: Thanks for your suggestion, which has been considered within the next draft. Rather than remove it, the IDT reworded the clause, but not the meaning or substance, so that it now reads, "(i.e., a Critical Asset cannot function as intended without the		

Organization	Yes or No	Question 5 Comment
Cyber Asset)"		
Ingleside Cogeneration LP	Yes	We commend the Interpretation Drafting Team for developing a reading of the term "essential" based upon its commonly understood usage. We also agree that it is important to provide gradations which are close to the concept of essentiality, but does not meet the criticality litmus test. This allows the exclusion of Cyber Assets which "may be used, but not required" or are "merely valuable" to the inherent operation of the Critical Asset. It is left up to the Responsible Entity to make those assessments using an internal methodology that is comprehensive and defensible - and is consistent with the intent of CIP-002 as it is written today. We realize this flexibility may be limited in CIP version 5. However, those standards must still go through the vetting process; which will allow the industry to review, post comments, and vote upon any proposed changes.
Response: Thanks for support and supporting rationale for this interpretation.		
Tampa Electric Company	Yes	Tampa Electric agrees with the Interpretations Drafting Team response to Question 2. We strongly support the concept that essential to the operation of the Critical Asset means that it is necessary for the operation of that Critical Asset.
Response: Thanks for your strong support.		
Midwest ISO	Yes	MISO generally agrees with the Interpretation as to Question 2, however MISO also requests that the Interpretation Drafting Team clarify that "essential," as used in Requirement R3, is synonymous with "inherent", "necessary" and "required". MISO also submits that Registered Entities are best qualified to determine whether a Cyber Asset is essential to the operation of a CA and is therefore a CCA pursuant to the clarification provided by the Interpretation. As a result, a Registered Entity's determination of whether a Cyber Asset is required by a CA should be rebuttably presumed to be correct.

Organization	Yes or No	Question 5 Comment
Response: Thanks for your provided rationale. As the majority of industry agreed with this balloted draft's current explanation of essential, we see a greater risk in accepting the proposed change compared to leaving the words as currently written. Further, we agree with the MISO commenting body's final conclusion.		
Northeast Power Coordinating Council	Yes	
ISO/RTO Council Standards Review Committee	Yes	
Dominion	Yes	
Imperial Irrigation District (IID)	Yes	
Tennessee Valley Authority	Yes	
PacifiCorp	Yes	
Southern Company	Yes	
NIPSCO	Yes	
American Transmission Company, LLC	Yes	
Minnesota Power	Yes	
American Electric Power	Yes	
Independent Electricity System Operator	Yes	

Organization	Yes or No	Question 5 Comment
Ameren	Yes	
United Illuminating Company	Yes	
Salt River Project	Yes	
Pepco Holdings Inc	Yes	
City of Austin dba Austin Energy	Yes	
Essential Power, LLC	Yes	
Oncor Electric Delivery Company	Yes	
E.ON CLIMATE & RENEWABLES	Yes	
MidAmerican Energy Co.	Negative	See MidAmerican comments
Southwest Power Pool Regional Entity	No	The response to Question 2 must be revised to specifically include the proviso that redundancy is NOT a consideration when determining if a Cyber Asset is "essential." Redundancy cannot be a consideration because, generally, vulnerability of the reduntant asset is the same as the primary asset's vulnerability. To achieve security you have to consider both primary and redundant assets. The interpretation must also incorporate the provisions of CAN-0005 in such a way as to make CAN-0005 no longer necessary.
Response: While the IDT understands this particular rationale to be more in keeping with CAN-0005 and possibly forth-coming CIP versions, the IDT is bound by the Guidelines for Interpretation Drafting teams to interpret the words on the page of any standard		

Organization	Yes or No	Question 5 Comment
being interpreted. The IDT believes that incorporating the submitted suggestions would expand the scope of the requirement in question. Furthermore, the IDT understands that the interpretation, once approved, may result in withdrawal of CAN-0005. **The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this interpretation does not change that notion.**		
MidAmerican Energy Company	No	MidAmerican Energy does not believe this interpretation is needed at this time. The request is seeking the definition for the term "essential." Essential is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better defining this term either in an interpretation or in the NERC Glossary of Terms. The interpretation provides no new useful information and creates more confusion by introducing the new term "inherent to."
Response: The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities. The phrase "inherent to" in the interpretation is contextual and clarifying information, and the IDT disagrees that it is a new term.		
ReliabilityFirst	No	The Interpretation's "Response to Question 2" may render CIP-002-3 through CIP-009-3 non-functional. The statement, "A Cyber Asset that 'may' be used, but is not 'required' (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not 'essential to the operation of the Critical Asset' for purposes of Requirement R3" transforms CIP-002-3 R3 into a single point of failure analysis. Cyber systems used in the operation of the BES are designed so there is no single point of failure. Therefore, there would be no Critical Cyber Assets in the meaning stated by the "Response to Question 2."The Interpretation must be revised to make clear that any Cyber Asset, even if replicated locally or remotely, that, if damaged, lost or compromised, can have a negative impact on the reliable operation of the associated Critical Asset must be identified as a Critical Cyber Asset.
Response: The IDT agrees that redundancy is not a consideration in determining whether a Cyber Asset is "essential," and this		

Organization	Yes or No	Question 5 Comment
interpretation does not change that notion.		
CRSI	No	The definition provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. The interpretation does not provide additional clarity than what is provided in the existing guideline.
Response: Thanks for your rationale. The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation's response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.		

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard

Date submitted: 1/31/10

Date revised version submitted: 7/22/10

Contact information for person requesting the interpretation:

Name: Kim Long

Organization: Duke Energy Corporation

Telephone: 704-382-7179

E-mail: kim.long@duke-energy.com

Identify the standard that needs clarification:

Standard Number (include version number): CIP-002-1

(example: PRC-001-1)

Standard Title: Cyber Security – Critical Cyber Asset Identification

Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement: CIP – 002-1, Requirement R3

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

Clarification needed:

With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following:

1. Is the phrase "***Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange"*** meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be *assessed* for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
2. What does the phrase, ***"essential to the operation of the Critical Asset"*** mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
    - *The term "essential" is not defined in the NERC Glossary. T*he Merriam –Webster dictionary provides the following definition of essential: "**ESSENTIAL** implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character." The dictionary provides the following synonyms for essential: "Inherent, basic, indispensible, vital, fundamental, and necessary."

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

If the phrase 'Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control' is meant to be prescriptive such that workstations, which are utilized in monitoring and control must be classified as Critical Cyber Assets, then the ability to provide remote support is not available to companies.

It is inherently not possible to implement all of the prescribed controls, i.e. CIP 006 physical controls, around workstations such as laptops when used from remote locations. The reliability of the Bulk Electric System will be eroded, rather than enhanced, if companies do not have the ability to remotely access the Critical Asset environment by utilizing laptop workstations with the cyber security controls prescribed in CIP 005.

Interpretation 2010-INT-05: Response to Request for an Interpretation of NERC Standard CIP-002-1 R3 for the Duke Energy Corporation

The following interpretation of NERC Standard CIP-002-1 Cyber Security — Critical Cyber Asset Identification was developed by a sub team of the Cyber Security Order 706 Standard Drafting Team.

Requirement Number and Text of Requirement

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a control center; or,
R3.3. The Cyber Asset is dial-up accessible.

Question 1

Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?

Response to Question 1

The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.

Question 2

What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the

Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.

Response to Question 2

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Note: an Interpretation cannot be used to change a standard.

Request for an Interpretation of a Reliability Standard

Date submitted: 1/31/10

Date revised version submitted: 7/22/10

Contact information for person requesting the interpretation:

Name: Kim Long

Organization: Duke Energy Corporation

Telephone: 704-382-7179

E-mail: kim.long@duke-energy.com

Identify the standard that needs clarification:

Standard Number (include version number): CIP-002-1

(example: PRC-001-1)

Standard Title: Cyber Security – Critical Cyber Asset Identification

Identify specifically what requirement needs clarification:

Requirement Number and Text of Requirement: CIP – 002-1, Requirement R3

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

Clarification needed:

With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following:

1. Is the phrase "***Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange"*** meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be *assessed* for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
2. What does the phrase, ***"essential to the operation of the Critical Asset"*** mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.
    - *The term "essential" is not defined in the NERC Glossary. T*he Merriam –Webster dictionary provides the following definition of essential: "**ESSENTIAL** implies belonging to the very nature of a thing and therefore being incapable of removal without destroying the thing itself or its character." The dictionary provides the following synonyms for essential: "Inherent, basic, indispensible, vital, fundamental, and necessary."

Identify the material impact associated with this interpretation:

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

If the phrase 'Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control' is meant to be prescriptive such that workstations, which are utilized in monitoring and control must be classified as Critical Cyber Assets, then the ability to provide remote support is not available to companies.

It is inherently not possible to implement all of the prescribed controls, i.e. CIP 006 physical controls, around workstations such as laptops when used from remote locations. The reliability of the Bulk Electric System will be eroded, rather than enhanced, if companies do not have the ability to remotely access the Critical Asset environment by utilizing laptop workstations with the cyber security controls prescribed in CIP 005.

Interpretation 2010-INT-05: Response to Request for an Interpretation of NERC Standard CIP-002-1 R3 for the Duke Energy Corporation

The following interpretation of NERC Standard CIP-002-1 Cyber Security — Critical Cyber Asset Identification was developed by a sub team of the Cyber Security Order 706 Standard Drafting Team.

Requirement Number and Text of Requirement

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a control center; or,
R3.3. The Cyber Asset is dial-up accessible.

Question 1

Is the phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity’s critical cyber asset methodology?

Response to Question 1

The phrase “Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange” is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types.

Question 2

What does the phrase, "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the

Critical Asset"? Remote access to the systems is valuable to operations (see Material Impact Statement below), but operation of the Critical Asset is not literally dependent on these laptops.

Response to Question 2

The word "essential" is not defined in the *Glossary of Terms used in NERC Reliability Standards*, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.

A Cyber Asset that "may" be used, but is not "required" (i.e., ~~without which~~ a Critical Asset cannot function as intended without the Cyber Asset), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3

3. Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-3:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballots Open

April 20 – 30, 2012

Project 2009-26 Interpretation of CIP-004-X for WECC

Project 2010-INT-05 Interpretation of CIP-002-X for Duke

Recirculation ballot periods are now open through **8 p.m. Eastern on April 30, 2012**

Now Available: Project 2009-26 | Project 2010-INT-05

Recirculation ballots for the interpretation of CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke are being conducted through **8 p.m. Eastern on April 30, 2012.**

The CIP-004-X Interpretation Drafting Team did not make any changes to the interpretation following the posting that ended on March 23, 2012.

The CIP-002-X Interpretation Drafting Team made a minor clarifying change in the Question 2 response by replacing the phrase, "without which" with the phrase "without the Cyber Asset" in the parenthetical as shown below:

- A Cyber Asset that "may" be used, but is not "required" (i.e., ~~without which~~ a Critical Asset cannot function as intended without the Cyber Asset) for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3.

A clean version of the interpretation for CIP-004-X has been posted on the project webpage and a clean and redline version of the interpretation for CIP-002-X has been posted on the project webpage.

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's last vote cast in the previous ballot will be carried over.

Next Steps

Voting results will be posted and announced after the ballot window closes. If approved, the interpretation(s) will be submitted to the Board of Trustees.

Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP Interpretations were developed by a drafting team consisting of a different group of members of the CIP Interpretation Drafting Team. Each team has reviewed all comments submitted in the previous posting of its interpretation, along with FERC orders issued since the previous posting, and responded to comments consistent with guidance adopted by the NERC Board of Trustees and the Standards Committee.

Information about the CIP Interpretation Drafting Team is available on the team's webpage, which contains links to each of the interpretations that the team is working on including the two being balloted now.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development and interpretation processes. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-26 Interpretation of CIP-004-X for WECC

Project 2010-INT-05 Interpretation of CIP-002-X for Duke Energy

Recirculation Ballot Results

Project 2009-26: Now Available
Project 2010-INT-05: Now Available

Recirculation ballots for the interpretation of CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke both concluded April 30, 2012.

Voting statistics for the ballots are listed below, and the Ballot Results page provides a link to the detailed results.

Standard	Quorum	Approval
CIP-004-X - Cyber Security – Personnel and Training for WECC	Quorum: 90.96%	Approval: 80.08%
CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke	Quorum: 92.68%	Approval: 94.61%

Next Steps
CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke will be presented to the NERC Board of Trustees for adoption and subsequently filed with regulatory authorities.

Background
Additional information is available on the project pages.
Project 2009-26 and Project 2010-INT-05

Standards Development Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica

Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

Ballot Results

Ballot Name:	Project 2010-INT-05 CIP-002-1 R3 for Duke Energy
Ballot Period:	4/20/2012 - 4/30/2012
Ballot Type:	recirculation
Total # Votes:	304
Total Ballot Pool:	328
Quorum:	**92.68 % The Quorum has been reached**
Weighted Segment Vote:	94.61 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	82	1	70	0.972	2	0.028	9	1
2 - Segment 2.	10	0.7	7	0.7	0	0	2	1
3 - Segment 3.	77	1	65	0.985	1	0.015	5	6
4 - Segment 4.	23	1	21	1	0	0	1	1
5 - Segment 5.	75	1	58	0.983	1	0.017	7	9
6 - Segment 6.	44	1	35	0.972	1	0.028	4	4
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.8	7	0.7	1	0.1	0	0
9 - Segment 9.	2	0.1	1	0.1	0	0	0	1
10 - Segment 10.	7	0.6	4	0.4	2	0.2	0	1
Totals	**328**	**7.2**	**268**	**6.812**	**8**	**0.388**	**28**	**24**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain	View

1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	View
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Abstain	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Negative	View
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Abstain	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Theresa Allard	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	View
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	

1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	View
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	View
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Ameren Services	Mark Peters	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Abstain	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	View
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Danny Lindsey	Affirmative	View
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	View
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Abstain	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	

3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen		
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson		
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	View
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Abstain	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	View
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	View
5	AEP Service Corp.	Brock Ondayko	Affirmative	View
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Colorado Springs Utilities	Jennifer Eckels	Abstain	

5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Abstain	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Affirmative	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	View
5	Essential Power, LLC	Patrick Brown	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh		
5	ICF International	Brent B Hebert	Abstain	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	View
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Abstain	
5	Puget Sound Energy, Inc.	Tom Flynn		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	View
5	Tacoma Power	Claire Lloyd	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Tri-State G & T Association, Inc.	Barry Ingold		
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	View
6	APS	RANDY A YOUNG	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	

6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Abstain	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Manitoba Hydro	Daniel Prowse	Affirmative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Powerex Corp.	Daniel W. O'Hearn		
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Abstain	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Affirmative	
8		James A Maenner	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	View
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Exhibit E

Roster of the Interpretation Drafting Team for the Interpretation of Requirement R3 of CIP-002-4 — Critical Cyber Asset Identification.

Interpretation 2010-INT-05
CIP-002-1 Requirement 3 for Duke Energy
Drafting Team Roster

Name and Title	Company and Address	Contact Info	Bio
Scott Miller, Chair Manager Corporate Affairs	MEAG Power 1407 Riveredge Parkway NW Atlanta, GA 30328	(678) 644-3524 smiller@meagpower.org	Mr. Miller actively works with American Public Power Association (APPA) and the Large Public Power Council (LPPC) Reliability Team to develop multi-company responses and positions on CIP standard developments as well as other NERC standards. He is an active member of the NERC Quality Review Team, and he has completed SOS NERC Training modules for relays, power plant operations, security, and other topics. Responsibilities include working on cyber issues that require the continual studying of cyber network and network security texts, and to monitor and review Congressional, FERC and NERC committee hearings, meetings and webinars. More than 30 years of electric and natural gas industry experience, which includes providing research, proposals, and testimony to FERC and the Illinois Commerce Commission as the primary liaison and witness on gas and electric rate making, engineering practices, and accounting/equipment life cycle studies. At MEAG Power, he provides 25 municipal electric distribution utilities with system planning and operational support. Mr. Miller has held various management and executive staff positions, and he is a USAF veteran and holds a BA and an MBA with an emphasis in numerical analysis. He is a member of the NERC CIP Interpretation Drafting Team.

Interpretation 2010-INT-05
CIP-002-1 Requirement 3 for Duke Energy
Drafting Team Roster

David Dockery NERC Reliability Compliance Coordinator	Associated Electric Cooperative, Inc. 2814 S Golden Ave Springfield, MO 65807	(417) 885-9286 ddockery@aeci.org	David Dockery has more than 30 years experience in implementing, upgrading and maintaining AGC/SCADA systems including full change-management documentation, coding down to the RTU Front-end communications device-drivers, and history of participation in specifying new EMS/SCADA delivery within NERC Reliablity and CIP standards, including computer network layout design. As AECI Operations Engineer, Mr. Dockery was involved in coordinating/evaluating transmisson outages and maintaining OASIS reservations support system, as well as support of NERC Reliability standards related to Eastern Interconnection. He is currently the NERC Reliability Compliance Coordinator for AECI. Education 1976 Graduate BSEE University of Arkansas 1977-1978 UA EE Graduate Assistant, taking Masters-level courses in Electrical Power Systems Modeling/Analysis, and Computer Programming and Architecture June 1980 - Wisconsin Extension course June 1980: Computer Techniques for Real-time Control and Monitoring of Power Systems (Cohn, Phadke, Stott, Wollenburg) April 1988 – IEEE/Power Engineering Society course: Electric Power System Operation and Control (Wollenburg) Oct 2008 - GeorgiaTech Extension: Power System Relaying: Theory and Operation (Ayoub, Meliopoulos)
Mark Engels Enterprise Technology Security & Compliance Director	Dominion 707 East Main Street Richmond, VA 23219	(804) 775-5263 mark.engels@dom.com	Mark Engels is the Enterprise Technology Security and Compliance Director at Dominion and has been with the company 33 years. Mr. Engels is formerly a member of NERC's Cyber Security Standard Education Team (CSSET), which created the compliance audit presentation used at three NERC sponsored 1200 standard workshops and created the compliance audit presentation used at 10 NERC sponsored CIP-002-1 through CIP-009-1 standard workshops. Mr. Engels is currently a member of NERC's Critical Infrastructure Protection Committee (CIPC), chair of the NERC Control System Security Working Group (CSSWG), chair of the NERC Cyber Attack Task Force, and a member of the Southeastern Electric Reliability Corporation (SERC) CIPC leadership committee. He is a member of the NERC CIP Interpretation Drafting Team.

Interpretation 2010-INT-05
CIP-002-1 Requirement 3 for Duke Energy
Drafting Team Roster

Summer Esquerre Manager, NERC Reliability Standards (CIP)	NextEra Energy P.O. Box 14000 Juno Beach, FL 33408	561-691-7171 Summer.Esquerre@fpl.com	Summer C. Esquerre, as the Critical Infrastructure Protection (CIP) Manager, NERC Reliability Standards for NextEra Energy, Inc.'s (NextEra's) Compliance and Responsibility Organization, works closely with the CIP-003 Senior Manager to oversee and monitor the implementation of NextEra's CIP sustainable compliance program. NextEra has Registered Entities in all eight NERC regions, and NextEra also has compliance responsibility for virtually all registered functions. Ms. Esquerre is also a member of the core team drafting the electric grid enterprise-wide risk management guideline, a team headed by the Department of Energy Office of Electricity Delivery and Energy Reliability. The purpose of the team is to develop a harmonized electric grid enterprise-wide risk management guideline, based on organization missions, investments and stakeholder priorities, to provide one voluntary guideline for an integrated organization-wide approach to management of cyber security risks, including operation of the electric grid and the evolving smart grid. The team also includes members from the National Institute of Standards and Technology's Smart Grid Interoperability Panel and Cyber Security Working Group, the Department of Homeland Security, NERC, and utilities. She holds a Master's Degree in Information Assurance from Norwich University, and is a Certified Information Systems Security Professional (CISSP) as well as Certified in Risk and Information Systems Control (CRISC).

Interpretation 2010-INT-05
CIP-002-1 Requirement 3 for Duke Energy
Drafting Team Roster

Jeffrey Fuller Senior Manager, Enterprise Security Services	Dayton Power and Light 1065 Woodman Drive Dayton OH 45432	(937) 331-4057 jeffrey.fuller@ddplin.com	Jeffrey Fuller is responsible for the management of the Enterprise Security department at his company, including cyber security, contract security, security incident response plans, risk assessments, and auditing activities. He has managed the Critical Infrastructure Protection (CIP) Program as well as industry SOX and PCI compliance requirements. Mr. Fuller is an active member of the NERC and RFC CIPC as well as an observer of the NERC Project 2008-06 SDT and other working groups. He brings a background that includes experience in IT, law enforcement, and compliance. He is a member of the NERC CIP Interpretation Drafting Team. Education: BS – Information Technology – WGU School of Police Staff and Command - NWU Certifications: Certified Information Systems Security Professional (CISSP) / Microsoft Certified Systems Engineer (MCSE) / Microsoft Certified Systems Administrator (MCSA) / Cisco Certified Network Associate (CCNA) / Microsoft Certified Desktop Support Technician (MCDST) / Microsoft Certified Trainer (MCT) / CompTIA Security+, Network+ and A+.
Michael Mertz Director of NERC Regulatory Compliance	PNM Resources 414 Silver Ave SW Albuquerque, NM 87158	(505) 241-0676 michael.mertz@pnmresources.com	Mike Mertz joined PNM Resources in 2010 where he is the Director of NERC Regulatory Compliance. In his role he is responsible for all NERC Reliability Standards Compliance and Critical Infrastructure Protection for two affiliate utilities held by PNM Resources, Public Service Company of New Mexico (PNM) and Texas New Mexico Power (TNMP). During his 15 year career in the energy industry he has been very active in industry and NERC standards development processes including with most recent roles as Chairman of the DNP3 Users group, a voting member of the NERC CIP Interpretation and Violation Severity Level Drafting Teams, NERC Critical Infrastructure Protection Committee, and the NERC Critical Asset and Critical Cyber Asset guideline drafting teams. Prior to his current role at PNM Resources, he was the Manger of Information Security for Southern California Edison. Mike holds undergraduate degrees in Biology and Computer Science, numerous professional information security and audit certifications (CISSP, CISA, CISM etc.), as well as a M.S. in Information Systems Security from Boston University.

Interpretation 2010-INT-05
CIP-002-1 Requirement 3 for Duke Energy
Drafting Team Roster

Hong Tang Control Systems Staff Engineer	CenterPoint Energy P.O. Box 1700 Houston, TX 77002	(713) 207-7930 hong.tang@centerpointenergy.com	Hong Tang has over 13 years of experience in the electric utility industry. Ms. Tang is a Control Systems Staff Engineer at CenterPoint Energy and has coordinated the CIP compliance program at the Transmission Control Center since 2009. She helped implement many of the NERC CIP Standards at the control center and has been actively involved in all the CIP audits, spot checks, and certifications. Her experience also includes 3 years conducting management and operational audits at gas and electric utilities for a major consulting company and over 10 years in Control Systems providing support for the Energy Management System used by Real-time Operations to monitor the Bulk Electric System for CenterPoint Energy. She currently participates in the CIP Working Group along with representatives from other NERC Registered Entities in the ERCOT Region and the Transmission Forum Security Practices Group serving as a security subject matter expert for peer reviews. She also provides comments and recommendations to CenterPoint Energy's Compliance group regarding voting positions on draft NERC Reliability Standards and interpretations that impact or potentially impact CenterPoint Energy. She received a Bachelor of Science degree in Electrical Engineering from the University of Houston in 1998 and a Master of Business Administration degree from Houston Baptist University in 2003. In addition, Ms. Tang is a registered Professional Engineer (PE) in the State of Texas.