

Comment Form for Interpretation of CIP-002-1, Requirement R3 for Duke Energy (Project 2010-05)

Please **DO NOT** use this form to submit 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 comment form must be completed by **October 8, 2010**. This is a 30-day formal comment period. The drafting team will provide a response to each comment submitted.

If you have questions please contact Howard Gugel at Howard.Gugel@nerc.net or by telephone at 609-651-2269.

Background Information

Initial Draft of Interpretation for CIP-002-1, Requirement R3

Duke Energy Corporation requested clarification on two phrases contained within Requirement R3. The first question asked for clarity on the use of the inclusion of “examples” in the following 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.” The second question asked for clarity on the word “essential” in the phrase, “. . . essential to the operation of the Critical Asset.”

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

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 is asking for clarity on the **meaning** of a requirement.

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

Comments:

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

The request **expands** the reach of the standard.

The request **does not expand** the reach of the standard.

Comments:

Comment Form for Interpretation of CIP-002-1, Requirement R3 for Duke Energy (Project 2010-05)

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.

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

Yes

No

Comments:

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.