

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	
<p>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:</p> <p>R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,</p> <p>R3.2. The Cyber Asset uses a routable protocol within a control center; or,</p> <p>R3.3. The Cyber Asset is dial-up accessible.</p> <p>Clarification needed: With regard to the above requirements, Duke Energy respectfully requests an interpretation as to the following:</p> <p>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”</p>	

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. The 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, indispensable, 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.