A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-3(i)b

3. Purpose: NERC Standards CIP-002-3(i)b 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(i)b 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(i)b, "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(i)b:

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: See Implementation Plan for the Revised Definition of "Remedial Action Scheme"

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. Remedial Action Schemes 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(i)b, 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(i)b 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

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	N/A	The responsible entity has not documented a risk-based assessment methodology to use to identify its Critical Assets as specified in R1.
R1.1.	LOWER	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
R1.2.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not consider all of the asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.
R1.2.1.	LOWER	N/A	N/A	N/A	N/A
R1.2.2.	LOWER	N/A	N/A	N/A	N/A
R1.2.3.	LOWER	N/A	N/A	N/A	N/A
R1.2.4.	LOWER	N/A	N/A	N/A	N/A
R1.2.5.	LOWER	N/A	N/A	N/A	N/A

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.6.	LOWER	N/A	N/A	N/A	N/A
R1.2.7.	LOWER	N/A	N/A	N/A	N/A
R2.	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.
R3.	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.
R3.1.	LOWER	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
R3.2.	LOWER	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
R3.3.	LOWER	N/A	N/A	N/A	A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
R4.	LOWER	N/A	The Responsible Entity does not have a signed and dated	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)’s annual	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
			record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets **or** the list of Critical Cyber Assets (even if such lists are null.)	approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets, nor 3) a signed and dated approval of 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"	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	Adopted by the NERC Board of Trustees	Update
3a	May 9, 2012	Interpretation of R3 for Duke Energy adopted by the NERC Board of Trustees	
3b	February 7, 2013	Interpretation of R1.2.5 for OGE adopted by the NERC Board of Trustees	
3b	March 21, 2013	FERC Order issued remanding interpretation of R3 for Duke Energy; interpretation removed from standard (previously Appendix 1)	
3(i)b	November 13, 2014	Adopted by the NERC Board of Trustees	Replaced references to Special Protection System and SPS with Remedial Action Scheme and RAS

Appendix 1

Project 2012-INT-05: Response to Request for an Interpretation of NERC Standard CIP-002-3 for the OGE Energy Corporation
Date submitted: 2/24/11
The following interpretation of NERC Standard CIP-002-3 Cyber Security — Critical Cyber Asset Identification, Requirement R1.2.5, was developed by a project team from the CIP Interpretation Drafting Team.
Requirement Number and Text of Requirement
R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets. R1.2. The risk-based assessment shall consider the following assets: R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
Identify specifically what requirement needs clarification (as submitted):
Requirement Number and Text of Requirement: CIP-002-3 R1.2.5 - Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. Clarification needed: Based on the text above, an auditor could apply this standard to the Smart Grid Advanced Meter Infrastructure (AMI) remote connect/disconnect functionality. While the AMI system is not designed to perform automatic load shedding of 300 MW it could be repurposed to shed an aggregate load of 300 MW or more. However, it is important to note that the AMI remote disconnect function is not used for under-voltage load shedding or under-frequency load shedding as a part of the region's load shedding program. The primary purpose of the AMI remote connect/disconnect function is to connect and disconnect individual retail electric customers from a central location rather than at the meter itself to enable substantial efficiency gains. OGE would like NERC to clarify that a company's SmartGrid AMI functionality, which may be able to disconnect 300+ MW of load, is not considered a system or facility critical to automatic load shedding

under a common control system capable of shedding 300 mw and therefore it should not be included in the Company's risk based methodology. OGE believes this clarification is appropriate because CIP-002-3 R1.2.5 was written to address under-voltage and under-frequency load shedding systems; SmartGrid AMI disconnect functionality pertains to neither.

Question Summary

OGE Energy Corporation seeks clarification on the meaning of CIP-002-3, Requirement R1.2.5 as it relates to "SmartGrid Advanced Meter Infrastructure (AMI) remote connect/disconnect functionality."

In its response, the Interpretation Drafting Team will answer whether a company's SmartGrid AMI functionality, which may be able to disconnect more than 300 MW of load, is considered a system or facility critical to automatic load shedding under a common control system capable of shedding 300 MW or more under CIP-002-3, Requirement 1.2.5.

Response

In evaluating OGE's request, the Interpretation Drafting Team (IDT) clarifies the meaning of CIP-002-3, Requirement R1.2.5 as it relates and applies to new technologies such as AMI. CIP-002-3, Requirement R1.2.5, along with the context of the standard as a whole, informed development of this interpretation.

CIP-002-3, Requirement R1.2 specifies that the Responsible Entity's risk-based assessment methodology ("RBAM") "shall consider" the assets described in Requirement R1.2.5.

During the identification and documentation of the RBAM, a Responsible Entity shall consider "Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more" as specified in Requirement R1.2.5. Requirement R2 then requires the entity to apply this RBAM annually to identify Critical Assets. If a system or facility does not meet the specifications of Requirement R1.2.5, the RBAM is not required to consider that asset.

The Critical Asset identification method under CIP-002-3, Requirement R1 is based on a facts and circumstance-driven analysis and is not dependent exclusively on specific technology or specific types of systems or facilities. For instance, systems or facilities such as AMI may have the potential or capability to be set up to automatically shed load, but having that potential or capability does not necessarily mean that the system or facility performs the function as described in Requirement R1.2.5. Therefore, an AMI system specifically built and configured to perform the Remote Disconnect function that does not automatically shed load without human operator initiation would not meet the criteria found in CIP-002-3, Requirement R1.2.5.