DIRECT TESTIMONY OF GREGORY D. ROWLAND FRANCHISED ELECTRIC AND GAS POLICY DEVELOPMENT DIRECTOR, DUKE ENERGY BUSINESS SERVICES LLC ON BEHALF OF DUKE ENERGY INDIANA, INC. CAUSE NO. 44367 BEFORE THE INDIANA UTILITY REGULATORY COMMISSION

I. INTRODUCTION

Q. PLEASE STATE YOUR NAME AND BUSINESS ADDRESS.

A. My name is Gregory D. Rowland and my business address is 550 South Tryon Street, Charlotte, NC 28202.

Q. BY WHOM ARE YOU EMPLOYED AND IN WHAT CAPACITY?

A. I am employed as Franchised Electric and Gas Policy Development Director, by Duke Energy Business Services LLC. Duke Energy Business Services LLC is a service company affiliate of Duke Energy Indiana, Inc. ("Duke Energy Indiana" or "Company").

Q. WHAT ARE YOUR RESPONSIBILITIES AS FRANCHISED ELECTRIC AND GAS POLICY DEVELOPMENT DIRECTOR?

A. My primary responsibility as Franchised Electric and Gas Policy Development Director is to provide leadership and direction in the development and advocacy of federal regulatory policy for Duke Energy's regulated generation and transmission businesses, with a focus on North American Electric Reliability Corporation ("NERC") policy and reliability standards. I work with our business units to develop policy positions that are consistent with our business objectives, which

include meeting our regulatory compliance obligations. I also lead Duke Energy's engagement in Federal Energy Regulatory Commission ("FERC") rulemakings on reliability standards and other issues to protect our policy positions.

Q. PLEASE DESCRIBE YOUR EDUCATIONAL AND PROFESSIONAL BACKGROUND.

A. I am a 1976 graduate of the University of South Carolina with a Bachelor of Science Degree in Electrical Engineering. Upon graduation, I was employed by E. I. DuPont de Nemours and Company, Inc. at the Savannah River Plant in Aiken, South Carolina, performing a variety of control systems engineering projects. I was employed by Duke Energy in 1978, initially designing relaying and metering modifications for coal-fired stations. Subsequently, I supervised strategic and business planning for the Research and Development area, which included research and economic studies of emerging power generation technologies. In the 1990's I led a group performing generation planning studies, which included electric industry restructuring studies. This ultimately led to my current role in 2002, evaluating and responding to a variety of FERC policy initiatives, including NERC's reliability standards.

Q. ARE YOU A REGISTERED PROFESSIONAL ENGINEER?

A. Yes, I am a registered Professional Engineer in the State of South Carolina.

Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY?

A. The purpose of my testimony is to describe the Critical Infrastructure Protection ("CIP") requirements that NERC has adopted and the FERC has approved. Specific

to this proceeding, I will discuss the NERC CIP Version 4 ("CIP 4") standards that are approved and discuss the penalties for non-compliance with the standards. I will also discuss the NERC CIP Version 5 ("CIP 5") standards that are pending at FERC. Finally, I will discuss Duke Energy Indiana's proposal to deal with confidential and highly sensitive information.

II. NERC CIP STANDARDS

Q. PLEASE PROVIDE SOME BACKGROUND REGARDING NERC'S ROLE IN SETTING AND ENFORCING RELIABILITY STANDARDS.

A. In 2005, a new Section 215 was added to the Federal Power Act which gave FERC jurisdiction to approve and enforce reliability standards requirements on all users, owners, and operators of the bulk power system. FERC certified NERC as the Electric Reliability Organization ("ERO"), and charged NERC with developing standards for FERC approval and enforcing approved standards with penalties for violations.

Q. PLEASE DESCRIBE THE EVOLUTION OF THE NERC CIP RELIABILITY STANDARDS VERSIONS 1-3.

A. On August 28, 2006, NERC submitted eight CIP Version 1 standards[1] for FERC approval. On January 18, 2008, FERC issued Order No. 706 approving Version 1, while directing NERC to make specific changes, including (1) removal of the "reasonable business judgment" language from each of the standards; (2) removal of the "acceptance of risk" exceptions from each of the standards; (3) development of

[1] CIP-002 through CIP-009-1

1 specific conditions that a Responsible Entity must satisfy to invoke the technical
2 feasibility exception; and (4) additional review and oversight regarding the creation
3 of the risk-based assessment methodology for critical cyber asset identification in
4 CIP-002-1. FERC also approved the phased compliance implementation plan, with
5 full compliance mandatory on July 1, 2010. FERC was concerned that allowing
6 Responsible Entities to interpret and apply the standards using "reasonable business
7 judgment" would unreasonably allow them to determine compliance with the
8 standards based upon their own business interests. FERC was also concerned that
9 the phrase "acceptance of risk" included in some requirements of the standards
10 would allow an entity to opt out of certain provisions at their own discretion. FERC
11 noted that while it was important to develop specific conditions needed to invoke a
12 technical feasibility exception, those conditions should not be limited to whether
13 something is technically possible, but whether it is technically safe and
14 operationally reasonable. Regarding the directive for additional review and
15 oversight of the creation of the risk-based assessment methodology, FERC stated
16 that external oversight would assure a wide area view and better ensure that
17 Responsible Entities identify appropriate assets as "critical."
18 On May 22, 2009, NERC filed the first phase of FERC-ordered
19 modifications to the eight NERC CIP Version 1 standards. The changes included
20 removing the terms "reasonable business judgment" and "acceptance of risk," and
21 other clarifying changes in response to FERC directives in Order No. 706. FERC
22 approved NERC CIP Version 2 on September 30, 2009, with an effective date of

April 1, 2010. FERC also directed NERC to make and file two additional specific changes: (1) modify CIP-006-2 to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit; and (2) remove a sentence from CIP-008-2 Requirement R1.6 which clarified that testing a Cyber Security Incident response plan need not include removing a system or component from service.

NERC submitted NERC CIP Version 3 on December 29, 2009, modifying NERC CIP-006-2 and CIP-008-2. NERC CIP Version 3 became effective on October 1, 2010. However, NERC CIP Versions 2 and 3 did not modify the critical asset identification process, which was a central FERC concern in Order No. 706.

Q. PLEASE DISCUSS CIP 4.

A. On February 10, 2011, NERC submitted CIP 4 for FERC approval. Although previous versions utilized a loosely-defined risk-based assessment methodology for determining critical assets, Version 4 contains a "bright line" Attachment 1 which describes specific uniform criteria for the identification of Critical Assets. These criteria are shown in Exhibit B-1 of my testimony. On April 19, 2012, FERC issued Order No. 761 approving CIP 4, with implementation required by April 1, 2014. On August 12, 2013, FERC granted an extension of time in which to comply with CIP 4 standards to October 1, 2014.[2] CIP 4 standards include:

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

CIP-003-4 – Cyber Security – Security Management Controls

[2] FERC stated that this extension would allow responsible entities to more efficiently utilize resources to transition directly from the currently-effective CIP 3 to the proposed CIP 5, if approved.

CIP-004-4 – Cyber Security – Personnel & Training

CIP-005-4 – Cyber Security – Electronic Security Perimeter(s)

CIP-006-4 – Cyber Security – Physical Security of Critical Cyber Assets

CIP-007-4 – Cyber Security – Systems Security Management

CIP-008-4 – Cyber Security – Incident Reporting & Response Planning

CIP-009-4 – Cyber Security – Recovery Plans for Critical Cyber Assets

These standards can be summarized as follows:

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

This standard 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. Critical Assets are to be identified in accordance with CIP-002-4 Attachment 1.

CIP-003-4 – Cyber Security – Security Management Controls

This standard requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

CIP-004-4 – Cyber Security – Personnel & Training

This standard requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

CIP-005-4 – Cyber Security – Electronic Security Perimeter(s)

1 This standard requires the identification and protection of the Electronic Security
2 Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access
3 points on the perimeter.

4 **CIP-006-4 – Cyber Security – Physical Security of Critical Cyber Assets**

5 This standard requires the implementation of a physical security program for the
6 protection of Critical Cyber Assets.

7 **CIP-007-4 – Cyber Security – Systems Security Management**

8 This standard requires Responsible Entities to define methods, processes, and
9 procedures for securing those systems determined to be Critical Cyber Assets, as
10 well as other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

11 **CIP-008-4 – Cyber Security – Incident Reporting & Response Planning**

12 This standard requires the identification, classification, response, and reporting of
13 Cyber Security Incidents related to Critical Cyber Assets.

14 **CIP-009-4 – Cyber Security – Recovery Plans for Critical Cyber Assets**

15 This standard requires that recovery plan(s) be put in place for Critical Cyber Assets
16 and that these plans follow established business continuity and disaster recovery
17 techniques and practices.

18 **Q. PLEASE DESCRIBE THE TYPES OF COMPLIANCE ACTIONS THAT**
19 **ARE REQUIRED UNDER CIP 4.**

20 A. The types of compliance actions include:

21 • Physical Security Perimeter ("PSP") - defining new boundaries and installing
22 necessary access control/monitoring mechanisms

- Electronic Security Perimeter ("ESP") - defining new boundaries and installing necessary access control/monitoring mechanisms
- Malicious Software Prevention - implementing tools/processes for the prevention of malicious code (viruses, *etc.*)
- Patching - implementing tools/processes for the application of security patches to mitigate known vulnerabilities
- Account Management - implementing tools/processes for the control/monitoring of individual and system access accounts on protected systems

I should point out that these same types of security measures were also required under NERC CIP Versions 1-3; however, CIP 4 increases the scope of assets to which these measures must be applied.

Q. DID DUKE ENERGY PARTICIPATE IN THE STANDARDS PROCESS AT NERC THAT RESULTED IN CIP 4?

A. Yes. Duke Energy has served on the NERC Standards Committee Process Subcommittee since 2010. The committee has focused on standards development process improvements to increase the quality and clarity of mandatory Reliability Standards and to enhance process efficiency. Since the issuance of FERC Order No. 693, Duke Energy has actively participated in the NERC standards development process on all new and revised reliability standards and allocates significant resources (both financial and human) to do so. A Duke Energy employee has served continuously since 2008 on the CIP standard drafting team in the development of CIP 2, 3, 4 and 5. In the NERC standards development process,

1 Duke Energy subject matter experts reviewed every draft of every CIP standard in
2 each version, submitted comments and suggestions for improvements, and voted in
3 every ballot. In the FERC proceedings, Duke Energy filed comments on the CIP
4 Version 1 NOPR, and participated in the development of EEI comments on CIP
5 Versions 2, 3, 4 and 5.

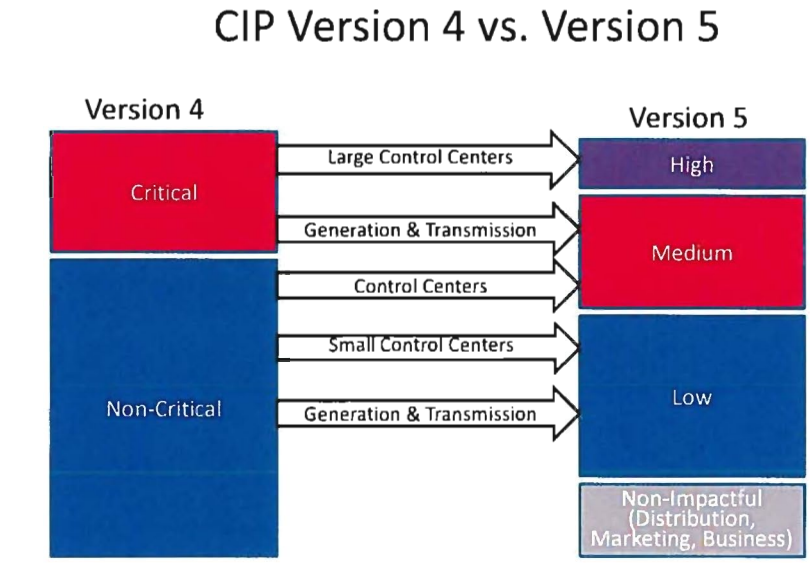
6 **Q. PLEASE DISCUSS CIP 5.**

7 A. On January 31, 2013, NERC submitted CIP 5 standards that are intended to address
8 all remaining FERC directives from Order No. 706. These changes include:

9 • Consideration of applicable features of the National Institute of Standards
10 and Technology ("NIST") Risk Management Framework, including
11 establishing CIP requirements based on entity functional characteristics
12 • Consideration of mechanisms for identifying Critical Cyber Assets by
13 examining all possible communication paths between a given cyber resource
14 and any asset supporting a reliability function
15 • Provision of a method for review and approval of Critical Cyber Asset lists
16 from external sources

17 CIP 5 utilizes a NIST-based approach to categorize all cyber systems that impact the
18 Bulk Electric System ("BES") as "High-Medium-Low." The biggest change from
19 CIP 4 is the inclusion of the Low Impact category which provides protection for
20 systems not included in CIP 4. In addition, CIP 5 includes the area of USB
21 Security, which entails implementing tools and processes for the appropriate use and

1 protection of thumb drives and other external media. The diagram below shows a
2 high level view of how CIP 4 and 5 are related.



Adapted from NERC "Cyber Security Standards Update Version 5"

3
4 NERC asked FERC to approve transitioning directly from Version 3 to CIP 5, with
5 a 24-month implementation timeframe for High and Medium Impact systems and a
6 36-month timeframe for Low Impact systems. CIP 5 is currently awaiting FERC
7 approval. We anticipate approval later this year with a compliance date of mid-
8 2015.

9 **Q. ARE THE TYPES OF SECURITY ACTIONS THAT YOU DESCRIBED**
10 **EARLIER FOR CIP 4 ALSO REQUIRED FOR CIP 5?**

11 A. Yes.

12 **Q. IS COMPLIANCE WITH CIP 4 MANDATORY FOR DUKE ENERGY**
13 **INDIANA?**

1 A. Yes. Compliance with CIP 4 is mandatory on the approved implementation
2 schedule unless and until modified by CIP 5.

3 **Q. ARE THERE PENALTIES FOR NON-COMPLIANCE WITH CIP 4?**

4 A. Yes. Non-compliance would result in financial penalties; however, the amount is
5 subject to variation. The penalties would be assessed by the regional entity
6 (Reliability*First* in Indiana), and approved by NERC and ultimately FERC. The
7 more flagrant the violation is or the more often they occur, the higher the penalties
8 become. Fines could be as high as $1M per day, per violation.

9 **Q. ARE THERE OTHER ACTIONS IN ADDITION TO COMPLIANCE WITH**
10 **CIP 4 THAT DUKE ENERGY INDIANA TAKES TO PROTECT ITS**
11 **ASSETS FROM CYBER ATTACKS?**

12 A. Yes. Compliance with CIP reliability standards is an important part of protecting
13 against cyber attacks. To augment and increase the effectiveness of the standards,
14 Duke Energy also monitors a variety of sources for threat and vulnerability
15 awareness in real-time. These include, but are not limited to the Department of
16 Homeland Security, the FBI, the Electric Sector – Information Sharing and Analysis
17 Center ("ES-ISAC"), National Electric Sector Cybersecurity Organization
18 ("NESCO"), NERC Alerts and other sources. Protective actions also include
19 vulnerability assessments, audits and incident responses.

20 **Q. HAS DUKE ENERGY INDIANA INCURRED OTHER EXPENSES THAT**
21 **ARE NOT INCLUDED IN THIS CASE IN ORDER TO COMPLY WITH**
22 **NERC STANDARDS?**

1 A. Yes. Following FERC Order No. 693, Duke Energy established its Electric
2 Reliability Executive Steering Committee to be responsible for providing oversight
3 of the electric reliability compliance program. The Steering Committee is
4 composed of executives from the various business units, and meets regularly to
5 review the effectiveness of the compliance program and provide strategic direction
6 for compliance with the NERC standards. Duke Energy's NERC Corporate
7 Compliance Team in the Ethics and Compliance Department provides independent
8 oversight for NERC reliability standards compliance activity across the company.
9 NERC Corporate Compliance manages a company compliance website that contains
10 program information and documents as well as compliance statements and evidence
11 documenting compliance with all NERC Reliability Standards and requirements.
12 Duke Energy's Generation and Transmission departments have added groups
13 responsible for managing compliance at the requirement level. The Information
14 Technology department also has a dedicated cyber security group. Together, these
15 groups consist of approximately 64 employees.

16 **III. <u>CONFIDENTIALITY AND SECURITY CONSIDERATIONS</u>**

17 **Q. ARE THERE SPECIAL CONFIDENTIALITY AND SECURITY**
18 **CONSIDERATIONS THAT NEED TO BE ADDRESSED CONCERNING**
19 **THE PROJECTS AT ISSUE IN THIS CAUSE?**

20 A. Yes. NERC Reliability Standard CIP-003-3 requires entities to implement and
21 document a program to identify, classify and protect information associated with
22 Critical Cyber Assets. Protected information includes, but is not limited to,

operational procedures, lists as required in CIP-002-X, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information. Furthermore, the Responsible Entity must document and implement a program for managing access to protected Critical Cyber Asset information.

Q. HAS DUKE ENERGY IMPLEMENTED AND DOCUMENTED A PROGRAM TO IDENTIFY, CLASSIFY AND PROTECT INFORMATION ASSOCIATED WITH CRITICAL CYBER ASSETS?

A. Yes. This requirement was part of CIP versions 1-3, and does not change in CIP 4.

Q. ARE THERE PENALTIES FOR FAILURE TO COMPLY WITH THESE RULES?

A. Yes. Failure of a Responsible Entity to follow its information protection program or access control program is a violation of the corresponding Reliability Standard requirements. Such violation exposes the Responsible Entity to NERC and FERC enforcement action, including the potential of monetary penalties.

Q. APART FROM THE PENALTIES, ARE THERE OTHER REASONS TO TREAT THE INFORMATION CONCERNING THE CIP 4 COMPLIANCE PROJECTS IN THIS CASE AS HIGHLY SENSITIVE CONFIDENTIAL INFORMATION?

A. Yes. If this information were to get into the hands of hackers or terrorists, for example, there could be great harm to the Bulk Electric System.

1 **Q. WHAT IS THE POTENTIAL HARM THAT COULD RESULT FROM**
2 **FAILURE TO TREAT THIS INFORMATION AS HIGHLY SENSITIVE**
3 **AND CONFIDENTIAL?**
4 A. For purposes of CIP 4, Critical Cyber Assets are those assets that are considered
5 essential to the operation of a Responsible Entity's Critical Assets. Critical Assets
6 are those assets which, if destroyed, degraded, misused, or otherwise rendered
7 unavailable, would affect the reliable operation of the Bulk Electric System,
8 potentially causing instability, uncontrolled separation or cascading outages. For
9 purposes of CIP 5, BES Cyber Assets are those assets that could adversely impact
10 the reliable operation of the Bulk Electric System. Therefore, identification of
11 Critical Cyber Assets and BES Cyber Assets must only be made on a need-to-know
12 basis, and must be protected against any further disclosure, to keep this information
13 away from potential attackers who could use it to harm the Bulk Electric System.
14 **Q. DO DUKE ENERGY INDIANA'S PROPOSED PROJECTS TO COMPLY**
15 **WITH CIP 4 AND 5 FALL UNDER THESE RULES?**
16 A. Yes. Duke Energy Indiana's projects which will be performed to comply with CIP
17 4 and 5 are directed towards Critical Cyber Assets and BES Cyber Assets identified
18 pursuant to methodologies specified in CIP-002-4 and CIP-002-5, respectively.
19 **Q. DOES THE INFORMATION PROVIDED IN THIS CASE NEED TO BE**
20 **TREATED IN A HIGHLY SENSITIVE AND SECURE MANNER?**
21 A. Yes. As previously discussed, the information about Critical Cyber Assets and BES
22 Cyber Assets in this case must be protected in order to prevent the information from

1 being obtained by groups or individuals who could potentially use the information
2 to harm the reliable operation of the Bulk Electric System.

3 **Q. HOW WILL THE COMPANY DEAL WITH INFORMATION REQUESTS**
4 **IN THIS CASE?**

5 A. First, each item of information requested will have to be evaluated to determine
6 whether provision of the information would violate NERC CIP Standards and/or
7 Duke Energy's Information Protection Program. Furthermore, the Company will
8 need to determine whether it is considered to be highly sensitive such that it could
9 cause harm to the Bulk Electric System if the information was not properly
10 protected, even if the information is not explicitly covered by NERC CIP or Duke
11 Energy's program. Based on these determinations, the Company may need to
12 restrict access to some information. Duke Energy Indiana commits to working with
13 the Commission, OUCC, and intervenors to provide the necessary information in
14 this case while also balancing confidentiality and security requirements.

15 **IV. CONCLUSION**

16 **Q. IN YOUR OPINION, ARE THE TYPES OF PROJECTS DISCUSSED BY**
17 **MR. ANDERSON AND MR. POWELL NECESSARY PARTS OF DUKE**
18 **ENERGY INDIANA'S PLAN TO COMPLY WITH CIP 4?**

19 A. Yes.

20 **Q. WAS PETIITONER'S EXHIBIT B-1 PREPARED BY YOU OR AT YOUR**
21 **DIRECTION?**

22 A. Yes.

Q. DOES THIS CONCLUDE YOUR PREPARED DIRECT TESTIMONY AT THIS TIME?

A. Yes.

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.

VERIFICATION

I hereby verify under the penalties of perjury that the foregoing representations are true to the best of my knowledge, information and belief.

Signed: Gregory D. Rowland Dated: 8-23-13

Gregory D. Rowland