



Registration Standards Applicability List for Joint Registration Organization (JRO) JRO00023

(Will be called Coordinated Functional Registration (CFR) when the proposed revision to the rules of procedure are passed.)

Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Member Entities

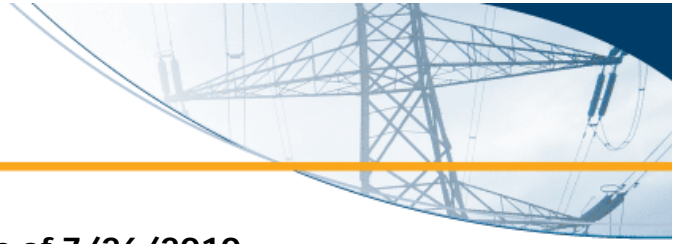
JRO Effective Registration Date

NCR00665 - AES Red Oak, L.L.C

2/6/2009

NCR10297 - TAQA Gen X LLC

2/6/2009



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: BAL-005-0.1b

Requirements:

R1. All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R1.1. Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-001-1

Requirements:

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-002-1

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.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-002-1

Requirements:

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-002-1

Requirements:

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

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

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

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.)

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-003-1

Requirements:

R1. Cyber Security Policy - The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Leadership - The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. The senior manager shall be identified by name, title, business phone, business address, and date of designation.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-003-1

Requirements:

R2.3. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. Exceptions - Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4. Information Protection - The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-003-1

Requirements:

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, 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.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-003-1

Requirements:

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendorrelated changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-004-1

Requirements:

R1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: Direct communications (e.g., emails, memos, computer based training, etc.); Indirect communications (e.g., posters, intranet, brochures, etc.); Management support and reinforcement (e.g., presentations, meetings, etc.).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.2.1. The proper use of Critical Cyber Assets;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-004-1

Requirements:

R2.2.3. The proper handling of Critical Cyber Asset information; and,

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-004-1

Requirements:

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-005-1

Requirements:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-005-1

Requirements:

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-005-1

Requirements:

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.1. A document identifying the vulnerability assessment process;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-005-1

Requirements:

R4.3. The discovery of all access points to the Electronic Security Perimeter;

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-006-1

Requirements:

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-006-1

Requirements:

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-006-1

Requirements:

R2.2. Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been peneled without authorization. These alarms must provide for immediate notification to personnel responsible for response.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-006-1

Requirements:

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-006-1

Requirements:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.3. The Responsible Entity shall document test results.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R5.3.1. Each password shall be a minimum of six characters.

Responsible Members:

NCR10297 TAQA Gen X LLC

NCR00665 AES Red Oak, L.L.C

R5.3.2. Each password shall consist of a combination of alpha, numeric, and “special” characters.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-007-1

Requirements:

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R8.1. A document identifying the vulnerability assessment process;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R8.3. A review of controls for default accounts; and,

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-008-1

Requirements:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-008-1

Requirements:

-
- R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-009-1

Requirements:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R1.2. Define the roles and responsibilities of responders.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: CIP-009-1

Requirements:

-
- R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: COM-002-2

Requirements:

- R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: EOP-004-1

Requirements:

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: EOP-004-1

Requirements:

- R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: IRO-001-1.1

Requirements:

- R8. Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: IRO-004-1

Requirements:

- R4. Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load-Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: PRC-001-1

Requirements:

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. Each Generator Operator shall coordinate all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5. A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the protection systems of others:

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R5.1. Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's protection systems.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: TOP-001-1

Requirements:

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R6. Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R7.1. For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R7.3. When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: TOP-002-2

Requirements:

R13. At the request of the Balancing Authority or Transmission Operator, a Generator Operator shall perform generating real and reactive capability verification that shall include, among other variables, weather, ambient air and water conditions, and fuel quality and quantity, and provide the results to the Balancing Authority or Transmission Operator operating personnel as requested.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R14.1. Changes in real output capabilities.

Responsible Members:

NCR10297 TAQA Gen X LLC
NCR00665 AES Red Oak, L.L.C

R15. Generation Operators shall, at the request of the Balancing Authority or Transmission Operator, provide a forecast of expected real power output to assist in operations planning (e.g., a seven-day forecast of real output).

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R18. Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers, and Load-Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3. Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: TOP-003-0

Requirements:

R1.1. Each Generator Operator shall provide outage information daily to its Transmission Operator for scheduled generator outages planned for the next day (any foreseen outage of a generator greater than 50 MW). The Transmission Operator shall establish the outage reporting requirements.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R2. Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC

R3. Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: TOP-006-1

Requirements:

R1.1. Each Generator Operator shall inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: VAR-002-1.1a

Requirements:

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings) as directed by the Transmission Operator.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.1. When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.1. A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC

R3.2. A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.

Responsible Members:

NCR00665 AES Red Oak, L.L.C
NCR10297 TAQA Gen X LLC



Registration Status as of 7/26/2010

Applicable Regional Entity: RFC

Applicable Function: GOP

Standard: VAR-002-1.1a

Requirements:

- R5.1. If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

Responsible Members:

NCR00665 AES Red Oak, L.L.C

NCR10297 TAQA Gen X LLC