PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 30, 2013

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP13-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID # NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Texas Reliability Entity, Inc. (Texas RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Texas RE's determination and findings of the violations[3] of CIP-002-1[4] R3 and R4; CIP-003-1 R1, R4, R5, and R6; CIP-004-1 R4; CIP-004-2 R3; CIP-

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

[4] The duration period of the violations included in this Full Notice of Penalty covers several Versions of the NERC Reliability Standards involved. For ease of reference, NERC is referring to the first applicable Version of these Standards but has listed all of the applicable Versions in the description of each violation.

005-1 R1, R4, and R5; CIP-006-1 R1; CIP-007-1 R1, R2, R3, R5, R7,[5] R8, and R9; CIP-008-1 R1; and CIP-009-1 R1, R2, R4, and R5.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred thirty-seven thousand dollars ($137,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers TRE201100424, TRE201100425, TRE201100426, TRE201100428, TRE201100429, TRE201100430, TRE201100431, TRE201100432, TRE201100433, TRE201100436, TRE201100437, TRE201100438, TRE201100446, TRE201100447, TRE201100448, TRE201100449, TRE201100450, TRE201100451, TRE201100452, TRE201100453, TRE201100454, TRE201100455, TRE201100457, and TRE201100458 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on March 1, 2013, by and between Texas RE and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

[5] The first applicable Version for the violation of R5 and R7 is CIP-007-2a.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Texas RE	Unidentified Registered Entity	NOC-1859	TRE201100424	CIP-002-1	3	High	$137,000
			TRE201100425	CIP-002-1	4	Lower	
			TRE201100426	CIP-003-1	1	Medium	
			TRE201100428	CIP-003-1	4	Medium	
			TRE201100429	CIP-003-1	5	Lower	
			TRE201100430	CIP-003-1	6	Lower	
			TRE201100431	CIP-004-1	4	Lower	
			TRE201100432	CIP-004-2	3	Lower	
			TRE201100433	CIP-005-1	1	Medium	
			TRE201100436	CIP-005-1	4	Medium	
			TRE201100437	CIP-005-1	5	Lower	
			TRE201100438	CIP-006-1	1	Medium	
			TRE201100446	CIP-007-1	1	Medium	
			TRE201100447	CIP-007-1	2	Medium	
			TRE201100448	CIP-007-1	3	Lower	
			TRE201100449	CIP-007-2a	5	Lower	
			TRE201100452	CIP-007-2a	7	Lower	
			TRE201100450	CIP-007-1	8	Lower	
			TRE201100451	CIP-007-1	9	Lower	
			TRE201100453	CIP-008-1	1	Lower	
			TRE201100454	CIP-009-1	1	Medium	
			TRE201100455	CIP-009-1	2	Lower	
			TRE201100457	CIP-009-1	4	Lower	
			TRE201100458	CIP-009-1	5	Lower	

CIP-002-1; CIP-002-2; CIP-002-3 R3 and R4 (TRE201100424 and TRE201100425)[6]

The purpose statement of Reliability Standard CIP-002-1 provides:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.
>
> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification - Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity[7] 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

[6] These violations cover Version 1 through Version 3 of this Standard. The language of CIP-002-2 and CIP-002-3 is different than the language of Version 1 of this Standard, as shown below.

[7] Within the text of the CIP Standards included in this Full Notice of Penalty, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

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:

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

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

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

CIP-002-1; CIP-002-2; CIP-002-3 R4 provide:

CIP-002-1 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.)

CIP-002-2 and CIP-002-3 R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP-002-1 R3 has a "High" Violation Risk Factor (VRF) and "High" Violation Severity Level (VSL). CIP-002-1 R4 has a "Lower" VRF and "Severe" VSL.

CIP-002-1; CIP-002-2; CIP-002-3 R3:
Texas RE conducted a Compliance Audit (Audit) of URE and found violations of the CIP Reliability Standards, which are included in this Full Notice of Penalty. The Audit Team determined that URE developed a list of Critical Cyber Assets (CCAs) essential to the operation of the Critical Asset list as per CIP-002-1 R2. However, prior to the Compliance Audit, there was no evidence to show that the subject list was reviewed or updated annually, as required by CIP-002-1 R3.

Auditor review of a document provided by URE did not provide sufficient evidence to demonstrate that the CCA list was annually reviewed or updated as necessary. The Critical Assets and CCAs lists were signed by URE's designated senior manager following the Texas RE Audit.

CIP-002-1; CIP-002-2; CIP-002-3 R4:
URE stated in its Reliability Standard Audit Worksheet (RSAW) that the URE senior manager or a delegate approves, on an annual basis, the risk-based assessment methodology (RBAM), the list of Critical Assets, and the list of CCAs. Texas RE determined during its review of a document that URE identified a person to serve as a senior manager. However, the senior manager's signature was not present on any of the CCA lists or Critical Asset lists submitted by URE for review. The evidence submitted did not have the dates or appropriate approval signatures pursuant to the NERC Standard or URE RBAM process.

The RBAM, Critical Assets list, and CCAs list were signed by URE's designated senior manager to demonstrate compliance following the Texas RE Audit.

Texas RE determined that URE had violations of CIP-002-1; CIP-002-2; and CIP-002-3 R3 and R4 because its lists of Critical Assets and CCAs were not reviewed and updated at least annually, and because URE's RBAM, Critical Assets list, and CCAs list were not signed by URE's designated senior manager prior to the Compliance Audit.

Texas RE determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE through when the Mitigation Plans were completed.

Texas RE determined that these violations posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). The moderate risk was

mitigated by the fact that the subject documents were implemented by URE and only lacked the necessary documented proof of annual review, documented signatures, and date.

CIP-003-1; CIP-003-2; CIP-003-3 R1, R4, R5, and R6 (TRE201100426, TRE201100428, TRE201100429, and TRE201100430)

The purpose statement of Reliability Standard CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of Standards numbered Standards CIP-002 through CIP-009."

CIP-003-1; CIP-003-2; CIP-003-3 R1 provide:

> 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:
>
> > R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
> >
> > R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
> >
> > R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

CIP-003-1 R4.1 provides:

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

CIP-003-1; CIP-003-2; CIP-003-3 R5.1, R5.2, and R5.3 provide:

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

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

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

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

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.

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

CIP-003-1; CIP-003-2; CIP-003-3 R6 provide:

> 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 vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R1.3 has a "Medium" VRF and a "Severe" VSL. CIP-003-1 R4.3 has a "Medium" VRF and a "Severe" VSL. CIP-003-1 R5.1.2, R5.2, and R5.3 have "Lower" VRFs and "Severe" VSLs. CIP-003-1 R6 has a "Lower" VRF and a "Severe" VSL.

CIP-003-1; CIP-003-2; CIP-003-3 R1:
During the Audit of URE, a review of URE's cybersecurity policy revealed that the cybersecurity policy was not approved by a senior manager and that the policy was not annually reviewed, pursuant to R1.3.

A signed and reviewed document was provided during the Audit, but a signed copy of URE's cybersecurity policy document was not provided. URE stated in the RSAW that as of the fall of 2010, URE determined that URE's generation facility was no longer a Critical Asset. Prior to that date, URE did have a cybersecurity policy for CIP-002-1 through CIP-009-1 that addressed each of the CIP requirements. The Audit Team determined that there was an initial review and approval of the cybersecurity policy but no annual review has been performed since URE took the generation facility off the Critical Asset list.

CIP-003-1; CIP-003-2; CIP-003-3 R4.3:
During the Audit, URE did not provide documentation pursuant to R4.3 to demonstrate that it had annually assessed adherence to its CCA information protection program, documented the assessment results, or implemented action plans to remediate any deficiencies. URE's cybersecurity policy provides that it has implemented and documented a program to identify, classify, and protect the information associated with its CCAs. CCA information to be protected includes, at a minimum and regardless of media type, operational procedures, and lists as required by Standard CIP-002.

URE's RBAM documents show that URE had determined that the generation facility was a Critical Asset prior to the fall of 2010. With the implementation of the new RBAM, the Critical Asset status of the facility changed and the facility was no longer a Critical Asset. However, the change was not approved and signed until during the Compliance Audit.

CIP-003-1; CIP-003-2; CIP-003-3 R5.2, and R5.3:
During the Audit, URE did not provide documentation pursuant to R5.2 to demonstrate that it annually reviewed the access privileges to protected information in order to confirm that the access privileges were correct. URE did not provide evidence pursuant to R5.3 that it annually assessed and documented the processes for controlling access privileges to protected information.

CIP-003-1; CIP-003-2; CIP-003-3 R6:
During the Audit, the Texas RE Audit Team observed during a walkthrough of URE's premises that a modem was not present physically but continued to be listed on the CCA lists. The Audit Team determined that the modem was physically removed, but was not removed from the CCA list, in violation of CIP-003-1 R6.

URE had a change control and configuration management program in place. The documents related to the program stated that URE's parent company will maintain a log of all configuration changes, but URE did not submit any log files as evidence during the Audit. Texas RE observed that some of the documents related to the program were not reviewed and updated annually, did not contain version control tables, or summaries with the review dates and approval dates. Texas RE's Audit Team determined that URE's documents regarding network change management, network configuration, router, switch and firewall confirmation were all unsigned, undated, and lacked version control language or tables.

The absence of configuration change logs and annual review evidence demonstrated URE's failure to implement supporting configuration management activities to identify, control, and document all entity-related or vendor-related changes to hardware and software components of CCAs pursuant to its change control process.

Texas RE determined that URE had violations of CIP-003-1; CIP-003-2; and CIP-003-3 R1, R4, R5, and R6 because its cybersecurity policy document was not annually reviewed and approved by a senior manager pursuant to R1.3; its RBAM changing Critical Asset status of the generation facility was not approved and signed pursuant to R4.3; URE

failed to review annually the access privileges to protected information to confirm that access privileges were correct, and failed to assess and document annually the processes for controlling access privileges to protected information, pursuant to R5.2 and R5.3; and failed to fully implement supporting configuration management activities to identify, control, and document changes to hardware and software components of CCAs pursuant to R6.

Texas RE determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE through when the Mitigation Plans were completed.

Texas RE determined that the violation of CIP-003-1 R1 posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, the absence of a managerial signature on the cybersecurity policy shows lack of management commitment to the policy. The absence of required signatures on numerous policies suggests more of a systemic issue versus an administrative oversight. However, the cybersecurity policy addressed the substantive requirements in Standards CIP-002 through CIP-009, and was readily accessible to all personnel responsible for CCAs.

Texas RE determined that the violation of CIP-003-1 R4.3 posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, the lack of documented assessment results of URE's adherence to its CCA information protection program, or the lack of implemented action plans to remediate any deficiencies, represent vulnerability in URE's CCA protection program. URE had no assessment data to determine if deficiencies existed. Moreover, absent a documented assessment, the safety of the CCA information was unknown, creating a risk that the information could be compromised. Lastly, the absence of required signatures on numerous policies suggests a systemic compliance issue. However, URE did have a documented program for treatment of CCA information that included the classification of information to be protected.

Texas RE determined that the violation of CIP-003-1 R5 posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, URE had a program for managing access to protected CCA information but the program was not fully implemented. The absence of annually documented assessments for controlling access privileges suggests that the access to protected information was unknown.

Texas RE determined that the violation of CIP-003-1 R6 posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, the risk was moderate because URE's change control and configuration management program implementation practices did not fully reflect its written program guidelines. The moderate risk was mitigated by the fact that URE had a change control and configuration management program, which was implemented and relied upon for the majority of URE's assets.

CIP-004-1; CIP-004-2; CIP-004-3 R4 and CIP-004-2; CIP-004-3 R3 (TRE201100431 and TRE201100432)

The purpose statements of Reliability Standard CIP-004-1; CIP-004-2; and CIP-004-3 provide in pertinent part:

> CIP-004 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. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.
>
> Standard CIP-004-2 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. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
>
> Standard CIP-004-3 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.
>
> Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

CIP-004-1; CIP-004-2; CIP-004-3 R4 provide:

> 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.
>
> > 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.
> >
> > 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

CIP-004-2 and CIP-004-3 R3 provide:

> 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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:
>
> > 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.

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.

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 Standards CIP-004-2 and CIP-004-3.

CIP-004-1 R4 has a "Lower" VRF and a "Severe" VSL. CIP-004-2 R3 has a "Lower" VRF and "Moderate" VSLs.

CIP-004-1; CIP-004-2; CIP-004-3 R4:
During the Audit, URE failed to provide evidence that it maintained a list of personnel with authorized cyber or authorized unescorted physical access to CCAs, as required by R4. URE provided evidence of quarterly reviews of physical access rights (R4.1) and a physical access revocation log (R4.2), but did not provide evidence of quarterly review of electronic access rights to CCAs.

URE had documentation for users that have shared accounts, which showed which personnel had specific electronic access rights. The personnel listed as having a common password to a shared account were reported to be the same personnel with electronic access rights.

URE only produced documentation for the second quarter for control room password changes to the shared account. Texas RE determined that this documentation was not sufficient to show compliance for the entire Audit period.

CIP-004-2; CIP-004-3 R3:
A review of URE's NERC background investigation policy and a sample of personnel risk assessments (PRAs) revealed that the background section of the background investigation policy did not include specific language stating that a PRA is required prior

to an individual being given authorized cyber or authorized unescorted physical access to CCAs.

The language of this background investigation policy reflected the requirements of CIP-004-1, which only required the PRA to be conducted within 30 days of such personnel being granted access. However, the subsequent Versions of CIP-004 required the PRA to be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances, such as an emergency. URE's policy was not updated during the Audit period to reflect this change but URE's actual hiring practices at the time reflected the Standard's intent.

Texas RE determined that URE had violations of CIP-004-1; CIP-004-2; CIP-004-3 R4 and CIP-004-2; and CIP-004-3 R3 because it failed to provide evidence that it maintained a list of personnel with authorized cyber or authorized unescorted physical access to CCAs; and because its policy did not include a requirement that a PRA needs to be completed prior to granting access to CCAs.

Texas RE determined the duration of the violation of CIP-004-1; CIP-004-2; and CIP-004-3 R4 to be from when the Standard became mandatory and enforceable to when the Mitigation Plan was completed. Texas RE determined the duration of the violation of CIP-004-2; and CIP-004-3 R3 to be from when the Standard became mandatory and enforceable to when the Mitigation Plan was completed.

Texas RE determined that the violation of CIP-004-2; and CIP-004-3 R3 posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, URE had an implemented background investigation policy during the pendency of the violation. URE's background investigation policy stated that all employees and vendors must successfully complete a background investigation prior to employment. URE was adhering to this requirement of its policy.

Texas RE determined that the violation of CIP-004-1; CIP-004-2; and CIP-004-3 R4 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE did review the electronic access rights to CCAs list, though not on a quarterly basis.

CIP-005-1; CIP-005-2; CIP-005-3; CIP-005-3a R1, R4, and R5.1 (TRE201100433, TRE201100436, and TRE201100437)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part:

> Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-005-1 R1 provides:

> 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).
>
> > 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).
> >
> > 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.
> >
> > 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).

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.

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.

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.

CIP-005-1 R4 provides:

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:

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

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

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

R4.4. A review of controls for default accounts, passwords, and network management community strings; and

> R4.5. 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.

CIP-005-1 R5 provides:

> 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.
>
> > R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP- 005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

CIP-005-1 R1 and R4 have "Medium" VRFs and "Severe" VSLs. CIP-005-1 R5.1 has a "Lower" VRF and a "Severe" VSL.

CIP-005-1; CIP-005-2; CIP-005-3; CIP-005-3a R1:
During the Audit, URE initially provided a Critical Asset list that failed to identify which assets on the list were CCAs. Later during the Audit, URE provided a revised list that included the critical labels.

The Audit Team noticed during its walkthrough examination of the URE facilities that the modem documented as a non-critical Cyber Asset was not present. The Audit Team also determined that an undocumented switch was present but not connected.

The Audit Team also reviewed additional evidence related to internet protocol addresses, which showed that the Cyber Assets residing in the Electronic Security Perimeter (ESP) were not identified and protected as required.

Texas RE determined that URE failed to identify all the access points to the ESP and maintain documentation of the ESP, of all interconnected critical and non-critical Cyber Assets within the ESP, and of all electronic access points to the ESP.

CIP-005-1; CIP-005-2; CIP-005-3; CIP-005-3a R4:
A review of URE's cyber vulnerability assessment (CVA) and the URE's parent company's security assessment report revealed that a CVA was not completed for the business network and plant network. During the following year, a partial CVA was completed on the business network, which did not include all the electronic access points to the ESP. URE did not submit any documentation to demonstrate that a CVA was completed in the two years. Further, because a CVA was not completed during the review period, the CVA could not address the minimum requirements of this Standard, including the discovery of all access point to the ESP.

CIP-005-1; CIP-005-2; CIP-005-3; CIP-005-3a R5.1:
During the Audit, Texas RE reviewed URE's CIP-005 policy, which revealed that CIP-005 policy and procedures were not being reviewed at least annually, in violation of R5.1.

Texas RE determined that URE had violations of CIP-005-1; CIP-005-2; CIP-005-3; and CIP-005-3a R1, R4, and R5.1 because it failed to identify all the access points to the ESP and maintain documentation of the ESP, all interconnected critical and non-critical Cyber Assets within the ESP, and all electronic access points to the ESP; because it did not have a CVA for the two years; and because its CIP-005 policy and procedures were not being reviewed at least annually.

Texas RE determined the duration of the violations to be from when the Standard became mandatory and enforceable for URE to when the Mitigation Plans were completed.

Texas RE determined that the violation of CIP-005-1; CIP-005-2; CIP-005-3; and CIP-005-3a R1 posed a minimal and not serious or substantial risk to the reliability of the BPS. While URE's Critical Asset list was not updated to reflect the status change of two devices, those devices were subsequently reported to be out of commission.

Texas RE determined that this violation of CIP-005-1; CIP-005-2; CIP-005-3; and CIP-005-3a R4 posed a moderate risk to the reliability of the BPS but did not pose a serious or substantial risk. Specifically, URE evaluated the enable statuses of the majority of URE's ESP access points and related ports and services. In addition, URE utilized CVA procedures to assess the vulnerability risk presented by the assess points within its ESP. URE's CVA procedures have been in place since the Standard became mandatory and enforceable.

Texas RE determined that this violation of CIP-005-1; CIP-005-2; CIP-005-3; and CIP-005-3a R5.1 posed a moderate risk to the reliability of the BPS but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's implementation and reliance upon its ESP security program. The EPS security program was utilized by URE but was not reviewed annually.

CIP-006-1; CIP-006-2; CIP-006-2a; CIP-006-3a; CIP-006-3c R1 (TRE201100438)

The purpose statement of Reliability Standard CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides in pertinent part:

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

CIP-006-2; CIP-006-2a; CIP-006-3a; CIP-006-3c R1 provide in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.7. Update of the physical security plan within thirty calendar days of the completion 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.

R1.8. Annual review of the physical security plan.

CIP-006-1 R1 has a "Medium" VSL and a "Severe" VRF.

During the Audit, a review of the URE's parent company's NERC-CIP-006 policy and URE's parent company's physical security policy revealed that these documents were not approved by senior management or delegate, in violation of R1. Also, no evidence was provided of an annual review per CIP-006-1 R1.9 and CIP-006-2 R1.8. In addition, URE failed to update its policy regarding Physical Security Perimeter (PSP) updates in accordance with the changes in the Standard's Versions. Standard CIP-006-1 required such updates within a 90-day period, and CIP-006-2; CIP-006-3 R1.7 require the updates to be completed within 30 days.

Texas RE determined that URE had a violation of CIP-006-1; CIP-006-2; CIP-006- 2a; CIP-006-3a; and CIP-006-3c R1 for failing to have its physical security plan approved by its senior manager; for failing to address annual review of the plan; and for failing to update the update time requirements included in R1.7.

Texas RE determined the duration of the violation to be from when the Standard became mandatory and enforceable for URE to when the Mitigation Plan was completed.

Texas RE determined that this violation of CIP-006-1; CIP-006-2; CIP-006-2a; and CIP-006-3a; CIP-006-3c R1 posed a moderate and not a serious or substantial risk to the reliability of the BPS. The moderate risk was mitigated by the fact that although the physical security plan did not include senior manager approvals or evidence of annual reviews, the plan had been implemented since the enforceable Standard date and addressed the requirements of the Standard.

CIP-007-1; CIP-007-2a; CIP-007-3 R1, R2, R3, R5, R7, R8, and R9 (TRE201100446, TRE201100447, TRE201100448, TRE201100449, TRE201100452, TRE201100450, and TRE201100451)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part:

> Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-007-1 provides in pertinent part:

> 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.

CIP-007-1 R2 provides:

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

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.

CIP-007-1 R3 provides:

R3. Security Patch Management - The Responsible Entity, both 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).

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.

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.

CIP-007-1; CIP-007- 2a; CIP-007-3 R5 provide:

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.

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.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

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.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

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.

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.

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

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).

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

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

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

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

CIP-007-2a R7 provides in pertinent part:

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement 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-005-2.

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

CIP-007-1 R8:

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:

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

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;

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

> 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.

CIP-007-1 R9 provides:

> 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.[8]

CIP-007-1 R1 and R2 have "Medium" VRFs and "Moderate" VSLs; R3, R5, and R8 have "Lower" VRFs and "Severe" VSLs; R7 has a "Lower" VRF and a "Severe" VSL; and R9 has a "Lower" VRF and a "High" VSL.

CIP-007-1; CIP-007-1-2a; CIP-007-3 R1:
During the Audit, Texas RE determined that parent company has a change control management policy that directs how changes to the IT infrastructure are managed. The change control management policy requires a risk assessment, an implementation plan, testing, and a rollback plan in the event an implementation fails. URE maintained this policy along with the procedures to comply with R1. During the last quarter, URE contracted a vendor, which agreed to provide IT servicing support for URE. However, no evidence was provided during the Audit to show that URE was in compliance with R1 between when this Standard became mandatory and enforceable, and the start of the vendor support contract. Before the vendor support contract became effective, no evidence was provided to show how URE was testing and upgrading the software under the vendor contract or implementing the security patches and updates. During the period of this violation, URE's internal IT department handled port and services maintenance for some of the applicable CAs but did not provide documentation to show compliance.

The Audit Team determined that the software updates and security patches for the first three quarters of the year were not provided by URE. As a result, Texas RE determined that URE did not update the vendor CCAs until the fourth quarter of the year.

[8] The subsequent Versions of this Standard require changes to be documented within 30 days.

CIP-007-1; CIP-007-1-2a; CIP-007-3 R2.3:
URE provided evidence that the vendor formally details the ports and services required for plant network CCA devices and configuration changes before installing or replacing them. All ports and services are enabled or disabled and are pre-configured for operation. However, on one of its firewalls, URE has allowed Telnet access to a device because one switch was unable to generate an authentication key needed to enable access. To limit risk, URE has allowed only business network IP addresses to connect to the device from outside the plant network. Texas RE determined that URE's documentation was insufficient to demonstrate that URE had action plans to remediate or mitigate this risk vulnerability for this device, in violation of R2.3.

CIP-007-1; CIP-007-2a; CIP-007-3 R3:
URE provided documentation created by the vendor of security patch updates installed and the test results of such updates. However, for the first three quarters of the year, documentation related to patch updates was not provided by URE. URE did not retain the vendor's support service for software updates and security patch updates until the fourth quarter of the year. Therefore, Texas RE determined that URE did not update and document its cybersecurity software patches for all CCAs within its ESP.

CIP-007-1; CIP-007-2a; CIP-007-3 R5:
During the Audit, Texas RE determined that URE provided documentation that detailed a process for technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. However, URE's procedure did not cover the access and control policy for shared accounts which are used by URE plant employees, in violation of R5.1. Furthermore, URE did not provide detailed evidence that identifies all user accounts that have electronic access to Critical Assets and CCAs.

The Audit Team also determined that URE's technicians used shared accounts to login to the plant network systems. All plant network CCAs systems shared the same password, which is not part of URE's access control procedure. Therefore, Texas RE determined that no accountability for managing these accounts was documented, in violation of R5.2.2 and R5.2.3.

Further, URE failed to provide evidence of system generated or manually generated detailed logs of individual user account access activity to Critical Assets and CCAs within the ESP for a minimum of ninety days. URE's system access control and use policy did

not provide information related to acceptable uses of administrator, shared, and other generic account privileges, including factory default accounts, as required by R5.2.

CIP-007-2a; CIP-007-3 R7.3:
During the Audit, the Audit Team determined that two modems were listed on the Cyber Assets list, but the URE employees did not know where these modems were located, which suggested they were previously disposed of or redeployed. Despite having documented procedures for asset disposal and redeployment, URE did not provide records to show how the two modems were disposed of or redeployed, in violation of R7.3.

CIP-007-1; CIP-007-2a; CIP-007-3 R8:
During the Audit, Texas RE determined that the 2010 URE plant CVA was incomplete because it only addressed the business network and failed to assess the plant network. As a result, URE was found to be in violation of R8.

A CVA was performed by a vendor, on behalf of URE, but only for the business network systems. Vulnerabilities were identified, and an issue regarding one firewall was not followed up by a supporting action plan that was formally addressed, documented, and acknowledged.

Therefore, Texas RE determined that URE was in violation R8.4 for a failure to keep documentation of the assessment results and have an action plan to remediate or mitigate identified vulnerabilities for its facility.

CIP-007-1; CIP-007-2a; CIP-007-3 R9:
During the Audit, Texas RE determined that documentation specified in Standard CIP-007 was not reviewed at least annually, as required by R9. URE conducted reviews and performed the required maintenance. However, no evidence was provided to show the required CIP-007 documents were annually reviewed.

Texas RE determined that URE had violations of CIP-007-1; CIP-007-2a; and CIP-007-3 R1, R2, R3, R5, R7, R8, and R9. URE failed to test and upgrade software or implementing security patches and updates; failed to have action plans to remediate or mitigate an identified vulnerability; failed to update and document its cybersecurity software patches for all CCAs within its ESP; failed to have a complete procedure for access authentication of, and accountability for, all user activity; failed to have an action plan

to remediate or mitigate certain identified vulnerabilities; failed to update and document its cybersecurity software patches for all CCAs within its ESP during a period of this violation; failed to identify all user accounts that have electronic access to Critical Assets and CCAs; failed to show how two modems were disposed of or redeployed; failed to have a complete CVA for its facility; and failed to review at least annually the documentation specified in Standard CIP-007.

Texas determined the duration of all CIP-007 violations, except for the violation of CIP-007-2a R7, to be from the date the Standard became mandatory and enforceable for URE through when the Mitigation Plans were completed. The violation of CIP-007-2a R7 was from the date the Standard became mandatory and enforceable for URE through when the Mitigation Plan was completed.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R1 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's implementation of its change control management policy that has been in place since the Standard became enforceable. The policy assesses whether significant changes with Cyber Assets within the ESP could adversely affect existing cybersecurity controls. Further, URE evaluated the Cyber Assets in its ESP an applied remedies or addressed areas of concerns for the majority of applicable Cyber Assets. The scope of this violation was limited to specific software updates.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R2.3 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. However, URE did not document a process to ensure the ports and services related to the specific devices that were not under a service contract during the period of this violation were enabled for normal and emergency operations. Additionally, the action plan to remediate or mitigate the vulnerability risk with one of its firewalls, which allowed access to a device because one switch was unable to generate an authentication key, was insufficient. The moderate risk was mitigated by URE's documented ports and services procedures that have been in place since the Standard became enforceable. Under these procedures, URE uses its security assessment report that details the ports and services required for plant network CCA devices and configuration changes before installing them. The report fulfilled its purpose by revealing vulnerabilities and providing recommendations.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R3 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by the application of automatic security patches from the Windows server update for the operating system and applications. For non-Microsoft updates, URE receives alerts from vendors and websites. In addition, on a quarterly basis a technician evaluates all the plant network computers in order to apply the security and Windows updates, to run a security assessment, to review event logs, and to change passwords.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R5 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's utilization of an established process for technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimizes the risk of unauthorized access.

Texas RE determined that the violation of CIP-007-2a and CIP-007-3 R7.3 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's documented and partially implemented asset disposal or redeployment policy, which has been in place since the Standard became mandatory and enforceable. Texas RE only identified asset disposal or redeployment issues with the two modems only, not with all devices included in the program.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R8 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's partial CVA, which revealed vulnerabilities that needed to be addressed.

Texas RE determined that the violation of CIP-007-1; CIP-007-2a; and CIP-007-3 R9 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The moderate risk was mitigated by URE's reliance upon the CIP-007 documents. The documents' change history suggests that they have been periodically reviewed. Further, a majority of the required CIP-007 documents have been in place since the Standard became mandatory and enforceable.

CIP-008-1; CIP-008-2; CIP-008-3 R1 (TRE201100453)

The purpose statement of Reliability Standard CIP-008-1 provides in pertinent part: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-008-1 provides in pertinent part:

> 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:
>
> > R1.1 - Procedures to characterize and classify events as reportable Cyber Security Incidents.
> >
> > R1.2 - Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
> >
> > 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.
> > R1.4 - Process for updating the Cyber Security Incident response plan within ninety[9] calendar days of any changes.
> >
> > R1.5 - Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
> >
> > 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.

[9] The subsequent Versions of this Standard require updates to be completed within 30 days.

CIP-008-1 R1 has a "Lower" VRF and a "Severe" VSL.

The URE's parent company's CIP-008 policy and URE cybersecurity incident response plan define the process to characterize and classify events as reportable cybersecurity incidents (R1.1), identify general response actions and incident response teams (R1.2), and the general process to report cyber incidents (R1.3). However, specific details were often lacking. No evidence was provided to show the policy has been maintained through periodic reviews and approvals. The documents lacked adequate updates to the incident response plan within 90 (under CIP-008-1) or 30 calendar days (under CIP-008-2 and CIP-008-3) due to process changes or lessons learned from the annual test or from an actual incident (R1.4). Neither document had a management-level signature or approval, nor was there any evidence of an annual review (R1.5). No evidence was submitted regarding an annual test of the incident response plan, as required by R1.6.

Texas RE determined that URE had a violation of CIP-008-1; CIP-008-2; and CIP-008-3 R1 because URE's documents lacked adequate updates to the incident response plan, documents did not have a management-level signature or approval, and there was no annual review conducted.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable through when the Mitigation Plan was completed.

Texas RE determined that this violation of CIP-008-1; CIP-008-2; and CIP-008-3 R1 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE has developed a cybersecurity incident response plan that addresses all of the substantive components required by R1.1 through R1.6, but had not maintained the plan in accordance with these requirements. URE's failure to maintain the policy had the potential of compromising the reliability of the BPS because the lack of policy updates could have resulted in URE personnel providing ineffective response and management of a cyber incident due to the personnel reliance on a dated policy.

CIP-009-1; CIP-009-2; CIP-009-3 R1, R2, R4, and R5 (TRE201100454, TRE201100455, TRE201100457, and TRE201100458)

The purpose statement of Reliability Standard CIP-009-1 provides in pertinent part: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster

recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-009-1 R1 provides:

> 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:
>
> > R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
> >
> > R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R2 provides:

> 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.

CIP-009-1 R4 provides:

> 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.

CIP-009-1 R5 provides:

> 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.

CIP-009-1 R1 has a "Medium" VRF and a "Moderate" VSL. CIP-009-1 R2, R4, and R5 have "Lower" VRFs and "Severe" VSLs.

CIP-009-1; CIP-009-2; CIP-009-3 R1:
A review of the URE parent company's disaster recovery plan, which was applicable to URE's facility, revealed that the URE parent company did not review this plan annually, as required by R1. Furthermore, units were still referenced in the plan although they had already been decommissioned.

CIP-009-1; CIP-009-2; CIP-009-3 R2:
URE provided no evidence of an annual exercise of the disaster recovery plan or the URE parent company's disaster recovery plan, as required by R2. URE stated that the disaster recovery plan was only in effect for eight months before URE's facility was no longer considered a Critical Asset, therefore, there was no annual exercise conducted. However, the officially signed and approved new RBAM, which led to the removal of URE's facility from the Critical Asset list, was not completed until during the Compliance Audit.

CIP-009-1; CIP-009-2; CIP-009-3 R4:
The URE parent company's disaster recovery plan lacked detail related to the responsible person or group, media, and locations in the backup and restoration process, as required by R4. Detailed backup and restoration procedures for each critical system and documentation related to equipment configuration settings or spare components were not provided during the Audit.

CIP-009-1; CIP-009-2; CIP-009-3 R5:
URE provided no evidence of an annual testing of its backup media. The URE parent company's disaster recovery plan states that a vendor provides the backup testing services. However, no documentation was submitted to support this assertion. The plan also lacked details related to responsible person and groups, media, and locations in the backup process. Detailed backup and restoration procedures for each critical system were also not submitted as evidence. URE stated in the RSAW that the recovery plan was only in effect for eight months before the facility was no longer considered a Critical Asset; therefore, there was no annual backup media test conducted. The official signed and approved RBAM which removed the Critical Asset determination, however, was not completed until during the Compliance Audit.

Texas RE determined that URE had violations of CIP-009-1; CIP-009-2; and CIP-009-3 R1, R2, R4, and R5 because it did not review its disaster recovery plan annually; had no

evidence of an annual exercise of the disaster recovery plan; did not include sufficient detail in its disaster recovery plan; and did not test its backup media annually.

Texas RE determined the duration of these violations to be from the date the Standard became mandatory and enforceable through when the Mitigation Plans were completed.

Texas RE determined that the violation of CIP-009-1; CIP-009-2; and CIP-009-3 R1 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to provide evidence that the policy had been reviewed and approved by senior management could compromise the reliability of the BPS if an employee relies on the plan that was not reviewed and lacked management's endorsement. However, URE had a disaster recovery plan that had been in place since this Standard became mandatory and enforceable, and URE was prepared to use it to address potential reportable events.

Texas RE determined that the violation of CIP-009-1; CIP-009-2; and CIP-009-3 R2 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to maintain the policy had the potential of compromising the reliability of the BPS because the lack of policy updates could have resulted in URE personnel's ineffective response and management of a disaster due to reliance on a dated policy. However, URE had a disaster recovery plan that had been in place since this Standard became mandatory and enforceable, and URE was prepared to use it to address potential reportable events.

Texas RE determined that the violation of CIP-009-1; CIP-009-2; and CIP-009-3 R4 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Despite URE's failure to include processes and procedures for the backup and storage of information required to successfully restore CCAs, its recovery plan had been in place since this Standard's enforceable date.

Texas RE determined that the violation of CIP-009-1; CIP-009-2; and CIP-009-3 R5 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Despite URE's failure to test its backup media at least annually, the essential data was being stored and no reports of lost or corrupted data have been discovered.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Texas RE has assessed a penalty of one hundred thirty-seven thousand dollars ($137,000) for the referenced violations. In reaching this determination, Texas RE considered the following factors:

(1) URE had an internal compliance program (ICP) at the time the violations occurred, which Texas RE considered a neutral factor;

(2) The violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;

(3) URE was cooperative throughout the compliance enforcement process;

(4) There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

(5) The violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and

(6) There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factor, Texas RE determined that, in this instance, the penalty amount of one hundred thirty-seven thousand dollars ($137,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[10]

CIP-002-1; CIP-002-2; CIP-002-3 R3 and R4 (TRE201100424 and TRE201100425)

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006372 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-002-1 R4 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006771 and was submitted as non-public information to FERC in accordance with FERC orders.

[10] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plans required URE's to:

1. Have URE's senior manager sign the RBAM, the Critical Asset list, and the CCA list;
2. Implement procedural changes to ensure that URE will document all compliance efforts related to URE's CIP-002 obligations. URE parent company has adopted the practice of signing all procedures as part of the revision approval process. Attestations for all future annual CIP-002 compliance procedure reviews and RBAM events will be recorded and maintained in URE's compliance files; and
3. Create a single CIP-002 internal compliance procedure for all URE parent company subsidiary and affiliated companies.

URE certified that TREMIT006372 and TREMIT006771 were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plans were completed.

CIP-003-1; CIP-003-2; CIP-003-3 R1, R4, R5, and R6 (TRE201100426, TRE201100428, TRE201100429, and TRE201100430)

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT008309 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-003-1 R4 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT008314 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-003-1 R5 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006373 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by

NERC. The Mitigation Plan for this violation is designated as TREMIT006374 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and
2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that TREMIT008309, TREMIT006373, TREMIT006374 and TREMIT008314 were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plans TREMIT008309, TREMIT006373, TREMIT008314 and TREMIT006374 were completed.

CIP-004-1; CIP-004-2; CIP-004-3 R4 and R3 (TRE201100431 and TRE201100432)
URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006774 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006773 and was submitted as non-public information to FERC in accordance with FERC orders.
URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and
2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plans were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plans TREMIT006774 and TREMIT006773 were completed.

CIP-005-1; CIP-005-2; CIP-005-3; CIP-005-3a R1, R4, and R5 (TRE201100433, TRE201100436, and TRE201100437)

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006375 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006378 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-005-1 R5 was submitted as complete to Texas RE. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006379 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and
2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plans were completed. URE submitted evidence of completion of its Mitigation Plans. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas verified that URE's Mitigation Plans were completed.

CIP-006-1; CIP-006-2; CIP-006-2a; CIP-006-3c R1 (TRE201100438)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006380 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and
2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plan was completed.

CIP-007-1; CIP-007-2a; CIP-007-3 R1, R2, R3, R5, R7, R8, and R9 (TRE201100446, TRE201100447, TRE201100448, TRE201100449, TRE201100452, TRE201100450, and TRE201100451)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006384-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006385-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006386 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006779 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-2a R7 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006780-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006387 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-007-1 R9 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006388 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and
2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plans were completed.

CIP-008-1; CIP-008-2; CIP-008-3 R1 (TRE201100453)

URE's Mitigation Plan to address its violation of CIP-008-1 R1 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006781 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and

2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plan was completed.

CIP-009-1; CIP-009-2; CIP-009-3 R1, R2, R4, and R5 (TRE201100454, TRE201100455, TRE201100457, and TRE201100458)

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006389 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-009-1 R2 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006390 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-009-1 R4 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006783 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-009-1 R5 was submitted to Texas RE as complete. The Mitigation Plan was accepted by Texas RE and approved by NERC. The Mitigation Plan for this violation is designated as TREMIT006784 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Use its RBAM to assess its Critical Assets and CCAs; and

2. Receive a signed attestation from a URE vice president stating that URE's facility was not a Critical Asset. Prior to the application of the new RBAM, URE's facility was its sole Critical Asset.

URE certified that the above Mitigation Plans requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, Texas RE verified that URE's Mitigation Plans were completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[11]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[12] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2013. The NERC BOTCC approved the Settlement Agreement, including Texas RE's assessment of a one hundred thirty-seven thousand dollar ($137,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE had a compliance program at the time the violations occurred, which Texas RE considered a neutral factor, as discussed above;
2. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;

[11] *See* 18 C.F.R. § 39.7(d)(4).
[12] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

3. Texas RE reported that URE was cooperative throughout the compliance enforcement process;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. Texas RE determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
6. Texas RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred thirty-seven thousand dollars ($137,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30 day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between Texas RE and URE;

   a. Disposition Document; Common Information, included as Addendum A to the Settlement Agreement;

   b. Disposition Document for TRE201100424 and TRE201100425, included as Addendum B to the Settlement Agreement;

   c. Disposition Document for TRE201100426, TRE201100428, TRE201100429 and TRE201100430, included as Addendum C to the Settlement Agreement;

   d. Disposition Document for TRE201100431 and TRE201100432, included as Addendum D to the Settlement Agreement;

   e. Disposition Document for TRE201100433, TRE201100436 and TRE201100437, included as Addendum E to the Settlement Agreement;

   f. Disposition Document for TRE201100438, included as Addendum F to the Settlement Agreement;

   g. Disposition Document for TRE201100446, TRE201100447, TRE201100448, TRE201100449, TRE201100452, TRE201100450, and TRE201100451, included as Addendum G to the Settlement Agreement;

   h. Disposition Document for TRE201100453, included as Addendum H to the Settlement Agreement;

   i. Disposition Document for TRE201100454, TRE201100455, TRE201100457, TRE201100458, included as Addendum I to the Settlement Agreement; and

b) Record documents for the violation of CIP-002-1 R3 (TRE201100424), included as Attachment b:

   i. URE's Mitigation Plan designated as TREMIT006372 for CIP-002-1 R31;
   ii. URE's Certification of Mitigation Plan Completion for CIP-002-1 R3;
   iii. Texas RE's Verification of Mitigation Plan Completion for CIP-002-1 R3;

c) Record documents for the violation of CIP-002-1 R4 (TRE201100425), included as Attachment c:

i. URE's Mitigation Plan designated as TREMIT006771 for CIP-002-1 R4;
ii. URE's Certification of Mitigation Plan Completion for CIP-002-1 R4;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-002-1 R4;

d) Record documents for the violation of CIP-003-1 R1 (TRE201100426):

i. URE's Mitigation Plan designated as TREMIT008309 for CIP-003-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-003-1 R1;

e) Record documents for the violation of CIP-003-1 R4 (TRE201100428), included as Attachment e:

i. URE's Mitigation Plan designated as TREMIT008314 for CIP-003-1 R4;
ii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R4;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-003-1 R4;

f) Record documents for the violation of CIP-003-1 R5 (TRE201100429), included as Attachment f:

i. URE's Mitigation Plan designated as TREMIT006373 for CIP-003-1 R5;
ii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R5;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-003-1 R5;

g) Record documents for the violation of CIP-003-1 R6 (TRE201100430), included as Attachment g:

i. URE's Mitigation Plan designated as TREMIT006374 for CIP-003-1 R6;
ii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R6;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-003-1 R6;

h) Record documents for the violation of CIP-004-1 R4 (TRE201100431), included as Attachment h:

i. URE's Mitigation Plan designated as TREMIT006774-1 for CIP-004-1 R4;
ii. URE's Certification of Mitigation Plan Completion for CIP-004-1 R4;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-004-1 R4;

i) Record documents for the violation of CIP-004-2 R3 (TRE201100432), included as Attachment i:

i. URE's Mitigation Plan designated as TREMIT006773 for CIP-004-2 R3;
ii. URE's Certification of Mitigation Plan Completion for CIP-004-2 R3;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-004-2 R3;

j) Record documents for the violation of CIP-005-1 R1 (TRE201100433), included as Attachment j:

i. URE's Mitigation Plan designated as TREMIT006375-1 for CIP-005-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-005-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-005-1 R1;

k) Record documents for the violation of CIP-005-1 R4 (TRE201100436), included as Attachment k:

i. URE's Mitigation Plan designated as TREMIT006378 for CIP-005-1 R4;
ii. URE's Certification of Mitigation Plan Completion for CIP-005-1 R4;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-005-1 R4;

l) Record documents for the violation of CIP-005-1 R5 (TRE201100437), included as Attachment l:

i. URE's Mitigation Plan designated as TREMIT006379 for CIP-005-1 R5;
ii. URE's Certification of Mitigation Plan Completion for CIP-005-1 R5;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-005-1 R5;

m) Record documents for the violation of CIP-006-1 R1 (TRE201100438), included as Attachment m:

i. URE's Mitigation Plan designated as TREMIT006380-1 for CIP-006-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-006-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-006-1 R1;

n) Record documents for the violation of CIP-007-1 R1 (TRE201100446), included as Attachment n:

i. URE's Mitigation Plan designated as TREMIT006384-1 for CIP-007-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R1;

o) Record documents for the violation of CIP-007-1 R2 (TRE201100447), included as Attachment o:

i. URE's Mitigation Plan designated as TREMIT006385-1 for CIP-007-1 R2;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R2;

iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R2;

p) Record documents for the violation of CIP-007-1 R3 (TRE201100448), included as Attachment p:

i. URE's Mitigation Plan designated as TREMIT006386 for CIP-007-1 R3;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R3;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R3;

q) Record documents for the violation of CIP-007-1 R5 (TRE201100449), included as Attachment q:

i. URE's Mitigation Plan designated as TREMIT006779 for CIP-007-1 R5;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R5;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R5;

r) Record documents for the violation of CIP-007-1 R8 (TRE201100450), included as Attachment r:

i. URE's Mitigation Plan designated as TREMIT006387 for CIP-007-1 R8;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R8;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R8;

s) Record documents for the violation of CIP-007-1 R9 (TRE201100451), included as Attachment s:

i. URE's Mitigation Plan designated as TREMIT006388 for CIP-007-1 R9;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R9;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-1 R9;

t) Record documents for the violation of CIP-007-2a R7 (TRE201100449), included as Attachment t:

i. URE's Mitigation Plan designated as TREMIT006388 for CIP-007-2a R7;
ii. URE's Certification of Mitigation Plan Completion for CIP-007-2a R7;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-007-2a R7;

u) Record documents for the violation of CIP-008-1 R1 (TRE201100453), included as Attachment u:

i. URE's Mitigation Plan designated as TREMIT006781-1 for CIP-008-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-008-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-008-1 R1;

v) Record documents for the violation of CIP-009-1 R1 (TRE201100454), included as Attachment v:

i. URE's Mitigation Plan designated as TREMIT006389-1 for CIP-009-1 R1;
ii. URE's Certification of Mitigation Plan Completion for CIP-009-1 R1;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-009-1 R1;

w) Record documents for the violation of CIP-009-1 R2 (TRE201100455), included as Attachment w:

i. URE's Mitigation Plan designated as TREMIT006390 for CIP-009-1 R2;
ii. URE's Certification of Mitigation Plan Completion for CIP-009-1 R2;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-009-1 R2;

x) Record documents for the violation of CIP-009-1 R4 (TRE201100457), included as Attachment x:

i. URE's Mitigation Plan designated as TREMIT006783 for CIP-009-1 R4;
ii. URE's Certification of Mitigation Plan Completion for CIP-009-1 R4;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-009-1 R4;

y) Record documents for the violation of CIP-009-1 R5 (TRE201100458), included as Attachment y:

i. URE's Mitigation Plan designated as TREMIT006784 for CIP-009-1 R5;
ii. URE's Certification of Mitigation Plan Completion for CIP-009-1 R5;
iii. Texas RE's Verification of Mitigation Plan Completion for CIP-009-1 R5; and

z) URE's Initial Audit Results, included as Attachment z.

A Form of Notice Suitable for Publication[13]

A copy of a notice suitable for publication is included in Attachment aa.

[13] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charlie.berardesco@nerc.net Derrick Davis Senior Corporate Counsel Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512-583-4923 (512) 233-2233 – facsimile derrick.davis@texasre.org Rashida Caraway* Manager, Compliance Enforcement Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4977 (512) 233-2233 – facsimile rashida.caraway@texasre.org	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director of Enforcement 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charlie.berardesco@nerc.net

Sonia C. Mendonça
Assistant General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Texas Reliability Entity, Inc.

Attachments