PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

March 27, 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, NCRXXXXX and NCRXXXXX in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2] URE is registered in the Reliability*First* Corporation (Reliability*First*) region, the Southwest Power Pool Regional Entity (SPP RE) region, and the Texas Reliability Entity, Inc. (Texas RE) (collectively referred to as the Regional Entities) region.

This Notice of Penalty is being filed with the Commission because the Regional Entities and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from the Regional Entities' determination and findings of the violations[3] of CIP-004-3 R3 and R4; CIP-005-3a R2 and R4; CIP-006-3c R1, R2, and R6; and CIP-007-3 R2, R3, R5, R6 and R8. According to the

[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.

Settlement Agreement, URE agrees and stipulates to the Settlement Agreement in its entirety[4] and has agreed to the assessed penalty of ninety thousand dollars ($90,000),[5] 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 RFC201000690, RFC201100769, RFC201100931, RFC201100933, RFC201100934, RFC201100935, RFC201100936, RFC201100948, RFC2011001078, RFC2011001079, RFC2011001081, RFC2011001082, SPP201000447, SPP201100518, SPP201100586, SPP201100589,[6] SPP201100588, SPP201100595, SPP201100591, SPP201100594, SPP201100612, SPP201100613, SPP201100615, SPP201100616, TRE201000205, TRE201100291, TRE201100368, TRE201100373, TRE201100374, TRE201100375, TRE201100379, TRE201100369, TRE201100371, TRE201100372, TRE201100376 and TRE201100377 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 entered into as of March 30, 2012, by and between the Regional Entities 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 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

[4] The facts are stipulated solely for the purpose of resolving the subject matter subject to the Settlement Agreement and do not constitute admissions or stipulations for any purpose other than URE's admission that the facts stipulated constitute violations of the above-referenced NERC Reliability Standards.
[5] URE agreed to pay a monetary penalty of $30,000 to Reliability*First*, $30,000 to SPP RE, and $30,000 to Texas RE, for a total of $90,000.
[6] The Settlement Agreement incorrectly lists a violation of SPP210000589.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
ReliabilityFirst, SPP RE, and Texas RE	Unidentified Registered Entity	NOC-1329	RFC201000690; SPP201000447; TRE201000205	CIP-007-3[7,8]	R5	Medium	$90,000
			RFC201100769; SPP201100518; TRE201100291	CIP-007-3	R6	Lower	
			RFC201100931; SPP201100586; TRE201100368	CIP-004-3	R3	Lower	
			RFC201100933; SPP201100589; TRE201100373	CIP-006-3c	R1	Medium	
			RFC201100934; SPP201100588; TRE201100374	CIP-006-3c	R2	Medium	
			RFC201100935; SPP201100595; TRE201100375	CIP-006-3c	R6	Lower	
			RFC201100936; SPP201100591; TRE201100379	CIP-007-3	R8	Lower	
			RFC201100948; SPP201100594; TRE201100369	CIP-004-3	R4	Lower	

[7] All violations listed in this Full Notice of Penalty and Settlement Agreement involve Version 1 through Version 3 of the applicable CIP Reliability Standards, except for CIP-006-3c R1, R2 and R6; CIP-004-3 R4; and CIP-005-3a R2 and R4. The violations of CIP-006-3c R1 and R2 involve Version 1 to Version 3c; the violations of CIP-006-3c R6, involve Version 2 to Version 3c; the violations of CIP-004-3 R4 involve only Version 3; and the violations of CIP-005-3a R2 and R4 involve Version 1 through Version 3a of the CIP Reliability Standards.

[8] For consistency, the Settlement Agreement and this Full Notice of Penalty reference the most recent version of the Reliability Standard and Requirement applicable to each violation. However, the Settlement Agreement references CIP-005-3, although CIP-005-3a became effective on February 2, 2011 and is the last applicable version of the Reliability Standard

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			RFC2011001078; SPP201100612; TRE201100371	CIP-005-3a	R2	Medium	
			RFC2011001079; SPP201100613; TRE201100372	CIP-005-3a	R4	Medium	
			RFC2011001081; SPP201100615; TRE201100376	CIP-007-3	R2	Medium	
			RFC2011001082; SPP201100616; TRE201100377	CIP-007-3	R3	Lower	

I. Self-Reported Violations

CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205)

The purpose statement of Reliability Standard CIP-007-3 provides: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-007-3 R5 provides, in pertinent part:

> Account Management - The Responsible Entity[9] 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.

[9] Within the text of the CIP Reliability 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.

> 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 RS and Standard CIP-004-3 Requirement R4.
>
> 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
>
> R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-3 R5 has a "Medium" Violation Risk Factor (VRF)[10] and a "Severe" Violation Severity Level (VSL).[11]

URE submitted Self-Reports for CIP-007-3 R5 to the Regional Entities.[12] First, URE reported that it discovered during an internal audit that it failed to change a password on a port classified as a non-critical Cyber Asset from the factory default password prior to placing that port into service, in violation of CIP-007-3 R5.2.1. Due to a process execution error, URE's security test incorrectly concluded that the password was a CIP-compliant password, when in fact it was not CIP-compliant. In addition, URE reported that it failed to change eight individual user account passwords within the required annual timeframe, in violation of CIP-007-3 R5.3.3. The users of these accounts overlooked the accounts during their annual password changes.

[10] CIP-007-3 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a "Lower" VRF. CIP-007-3 R5.1, R5.1.3, R5.2.1, R5.2.3 and R5.3.3 each have a "Medium" VRF. In the context of this case, the Regional Entities determined the violations related to R5.2.1, R5.3.3 and R5.1.2, and a "Medium" VRF was appropriate.
[11] CIP-007-3 R5, R5.1, R5.1.1, R5.1.3, R5.2, R5.2.2, R5.2.3 and R5.3 have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.
[12] URE submitted two Self-Reports to Reliability*First* and URE submitted a Self-Report to Texas RE and to SPP RE within the same week.

URE submitted two additional Self-Reports for violations of CIP-007-3 R5 to the Regional Entities.[13] URE reported that it failed to review user accounts in accordance with CIP- 007-3 R5 for 17 workstations that serve generation dispatch, and for one server. Specifically, URE failed to review access privileges on the user accounts in accordance with CIP-003-3 R5 and CIP-004-3 R4. URE failed to communicate the requirement to complete the user account reviews and failed to monitor the status of these reviews.

Finally, during a multi-regional Compliance Audit URE provided logs of user account access to Cyber Assets, but those logs did not include system users. These system user accounts are used by operators and are shared among multiple individuals. Because URE did not track these system users, it failed to generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days, in violation of R5.1.2.

During the multi-regional Compliance Audit, the Regional Entities also discovered that URE did not change one user password at least annually as required by CIP-007-3 R5.3.3. Specifically, URE did not change the password for over 13 months.

The Regional Entities determined that URE violated CIP-007-3 R5 for its failure to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and for its failure to minimize the risk of unauthorized system access.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-007-1 to the date URE completed its Mitigation Plan.[14]

The Regional Entities determined that these violations posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, the port at issue resides within an Electronic Security Perimeter (ESP) as a non-critical Cyber Asset, and does not directly control any Critical Assets. Additionally, access to URE's systems is protected by a multifactor authentication requirement.

[13] URE submitted a Self-Report to Reliability*First* and approximately three weeks later URE submitted a Self-Report to Texas RE regarding the same violation of CIP-007-3 R5.
[14] Each occurrence included in this violation had a different duration period.

Second, URE performed a system impact assessment and confirmed that the failure to change passwords for the eight individual user accounts did not cause an impact to its system. URE's failure to perform annual password changes did not present a high risk to the reliability of the BPS because these passwords passively expire, although not on an annual basis, and once they expire, the passwords must be reset to allow access.

Third, URE protects against cyber attacks through multiple layers of security. With regard to URE's failure to review user accounts on the 17 workstations or the system user accounts, redundancy in URE's server and workstation environments would require potential attackers to bypass multiple layers of control, including human observation. For example, the 17 workstations are located within a Physical Security Perimeter (PSP), and are visible to personnel and shift supervisors. The risk presented by the lack of an annual review of system user accounts was mitigated by URE's use of multiple controls protecting those accounts and Cyber Assets, including strict physical access controls.

CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291)

CIP-007-3 R6 provides:

> Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
> >
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.

> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-3 R6 has a "Lower" VRF[15] and a "Severe" VSL.[16]

URE submitted Self-Reports[17] for violations of CIP-007-3 R6 to the Regional Entities, stating that during an internal audit, it discovered several instances in which it failed to process cybersecurity logs and alerts, as required by CIP-007-3 R6.

URE's log management and incident alerting system (System) is managed by URE's Information Technology (IT) Cyber Security team. URE's System is designed to receive system events captured in local system logs, but the System requires effective business process controls and communications between the IT Cyber Security team and the URE business units in order to function. URE failed to implement some of these business process controls and communications and, as a result, local security logs were not sent to the System for log management and incident alerting. Because URE did not receive security logs in its System, it did not process the security logs, and failed to maintain records documenting its review of security logs, in violation of CIP-007-3 R6.

The Regional Entities determined that URE violated CIP-007-3 R6 for its failure to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity for all Cyber Assets in its ESP.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with ClP-007-1 to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk because the risk was mitigated by the following factors. First, URE's current implementation of firewalls, network-based intrusion and

[15] CIP-007-3 R6, R6.4 and R6.5 each have a "Lower" VRF. CIP-007-3 R6.1, R6.2 and R6.3 each have a "Medium" VRF.
[16] CIP-007-3 R6 and all of its subrequirements have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.
[17] URE submitted a Self-Report to SPP RE, to Texas RE, and to Reliability*First*.

detection systems, and antivirus solutions helped mitigate the risk posed by URE's failure to ensure security logging. All security threats detected by these measures are monitored by URE's operations center twenty-four hours a day, seven days a week.

Second, URE's operations center actively monitors and responds to a host of enterprise-wide security tools and controls, including network intrusion detection and prevention systems, host-based intrusion detection and prevention systems, antivirus software, and firewall alerting. Collectively, these controls provide the operations center with a view of network-based cybersecurity events. This view allows the operations center to identify any potentially disruptive network events and actual cybersecurity incidents before they impact systems related to the BPS.

CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368)

The purpose statement of Reliability Standard CIP-004-3 provides: "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-004-3 R3 provides, in pertinent part:

> 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.

CIP-004-3 R3.1 has a "Lower" VRF[18] and a "High" VSL.

URE submitted Self-Reports for CIP-004-3 R3 to the Regional Entities. URE reported that due to a database programming error, URE incorrectly verified a seven-year criminal check for 12 employees, and granted those 12 employees access to Critical Cyber Assets (CCAs). Of the 12 employees with improper access to CCAs, seven had access to CCAs in the Reliability*First* region, ten had access to CCAs in the SPP RE region, and five had access to CCAs in the Texas RE region.

URE uses an automated process to process background check reports that it receives from a third-party vendor. The automated process was designed with the assumption that reports from the vendor would reflect full background checks. However, the vendor returned only partial background check data for the 12 employees at issue, and URE erroneously recorded the background checks as complete.

The Regional Entities determined that URE violated CIP-004-3 R3 for its failure to ensure that the Personnel Risk Assessments (PRAs) for 12 employees included a seven-year criminal check.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-004-1 to the date by which URE reviewed background checks for affected personnel and ordered and completed new background checks, as per CIP-004-3 R3.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, most of the affected employees were long-time personnel, and some had received recent, paper-based background checks prior to URE's implementation of its current online background check program used to ensure CIP compliance. Second, all 12 employees had partial background checks completed, including identity verification, but not a seven-year criminal check. Third, all 12 employees ultimately received clear background checks, which identified no issues. Fourth, URE provided all 12 employees with CIP training prior to granting them access to its CCAs.

[18] CIP-004-3 R3 has a "Medium" VRF. CIP-004-3 R3.1, R3.2 and R3.3 each have a "Lower" VRF. In the context of this case, the Regional Entities determined the violations related to R3.1, and had a "Lower" VRF was appropriate.

CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373)

The purpose statement of Reliability Standard CIP-006-3c provides: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-006-3c R1 provides, in pertinent part:

> 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:
>
> > R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
> >
> > R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
> >
> > R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
> >
> > R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

CIP-006-3c R1 has a "Medium" VRF[19] and a "Severe" VSL.[20]

[19] CIP-006-3c R1, R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.6.1 and R1.6.2 each have a "Medium" VRF. CIP-006-3c R1.7 and R1.8 each have a "Lower" VRF.

URE submitted Self-Reports for CIP-006-3c R1 to the Regional Entities,[21] stating that it discovered that a single non-critical Cyber Asset – a frequency device – was connected to an ESP but was not located within an identified PSP, as required by CIP-006-3c R1.1.

URE submitted an additional Self-Report for a violation of CIP-006-3c R1 to Reliability*First* and SPP RE. URE submitted another Self-Report for a violation of CIP-006-3c R1 to Reliability*First*.[22] URE reported that it discovered three separate incidents in which it did not properly escort visitors as required by CIP-006-3c R1.6. Two incidents occurred at one of URE's facilities and involved URE employees failing to escort URE employee visitors for short periods of time during two meetings at the facility. The third incident involved an URE employee at another facility who did not have authorized unescorted access but was able to enter the facility because a door was not functioning properly.

Specifically, on one occasion an URE employee escort left an URE employee visitor unescorted for approximately one minute while he retrieved a manual from his desk. On another occasion, an URE employee escort left an URE employee visitor unescorted for a short period of time while he found another employee to troubleshoot a technical issue that occurred during a meeting.

On another instance, an URE employee who did not have approved unescorted access accessed a PSP as a result of a door strike plate that was not properly adjusted. URE's operations center received door alarms for the facility, and the URE employee at issue called the operations center shortly after to report the alarms. Although the employee had requested access to the PSP, URE had not yet granted the employee access. The employee accessed the PSP for a few minutes to perform scheduled work, and when the door opened, the employee assumed that URE had already granted him access to the PSP.

Additionally, during the multi-regional Compliance Audit, the Regional Entities discovered that URE failed to provide a six-wall border at one facility. URE declared the whole facility as a PSP, except for the reception area of the facility. URE disclosed at the Compliance Audit that it had recently discovered a breach in the six-wall border between a conference room and the reception

[20] CIP-006-3c R1 has an assigned VSL of either "High" or "Severe." All of the subrequirements of CIP-006-3c R1 have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.
[21] URE submitted a Self-Report to Reliability*First*, to SPP RE, and Texas RE.
[22] The incidents reported in these two Self-Reports did not occur in the Texas RE region.

area, which was located approximately 25 feet above ground. The breach consisted of an open area above the ceiling tile in the conference room.

The Regional Entities determined that URE violated CIP-006-3c R1 for its failure to document, implement, and maintain a physical security plan.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-006-1 to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, the Cyber Asset frequency device identified in two of the Self-Reports was located within a locked room immediately adjacent to the PSP, and was also protected by multiple layers of human observation.

Second, the employee visitors identified another Self-Reports could not have accessed the area of the facility that contains CCAs, which is protected by secure doors with access controls. URE left the employee visitors unescorted for very short periods of time, spanning from approximately one to five minutes. Additionally, the employee involved in the second incident had received training, had a PRA, and had access to other CCAs.

Third, the Regional Entities determined that the facility identified during the multi-regional Compliance Audit was otherwise very secure. URE had implemented parking lot security, a ten-foot deep pond around the building, card access entrances, double-door man traps protecting areas containing Cyber Assets, alarms, and other security provisions. With all of these security measures in place, it would have been difficult for an individual to breach the six-wall border opening or to gain access to any CCAs if the six-wall border were breached.

CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374)

CIP-006-3c R2 provides:

> Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

CIP-006-3c R2 has a "Medium" VRF and a "Severe" VSL.[23]

URE submitted Self-Reports for CIP-006-3c R2 to the Regional Entities, stating that it failed to monitor two firewalls that serve as access points to Cyber Assets that authorize or log access to PSPs. URE failed to identify the two firewalls as subject to the requirements of CIP-005-3 R3, as required by CIP-006-3c R2.2. URE did collect and retain firewall logs for the two firewalls for at least 90 days, but it did not perform all of the monitoring and alerting on the two firewalls required by CIP-005-3 R3. Specifically, URE did not detect and provide alerts for attempted, or actual unauthorized access to the two firewalls.

The Regional Entities determined that URE had violations of CIP-006-3c R2 for its failure to afford the protective measures specified in CIP-005-3 R3 to Cyber Assets that authorize and/or log access to the PSP.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-006-1 to the date that URE implemented the requisite monitoring and alerting on the two firewalls.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, the Cyber Assets behind the two firewalls (two Cyber Assets that authorize and log access to the PSPs) were protected in accordance with the other requirements of CIP-006-3c R2. These protections included residing within a PSP and having appropriate patches and password controls in place. Second, URE collected and retained firewall logs for the two firewalls for at least 90 days, and these logs did not reveal any unusual activity.

[23] CIP-006-3c R2 has an assigned VSL of "Severe." This is considered a binary requirement, where every violation is assigned a "Severe" VSL.

CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375)

CIP-006-3c R6 provides:

> Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
>
> - Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
> - Video Recording: Electronic capture of video images of sufficient quality to determine identity.
> - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

CIP-006-3c R6 has a "Lower" VRF and a "Severe" VSL.[24]

URE submitted Self-Reports for CIP-006-3c R6 to the Regional Entities,[25] stating that it reviewed its visitor logs and identified several instances in which it did not properly log visitor access to a PSP. The review of the visitor logs was conducted in response to compliance guidance from Reliability*First*.

Specifically, URE learned that it should log each entry and exit to and from a PSP. Prior to the issuance of the compliance guidance URE believed that CIP-006 only required it to log access at the initial entry and final exit for each individual, and URE did not log any interim entries or exits for each individual. Once URE learned the proper scope of this Standard, URE reviewed its visitor logs and identified instances in which it failed to log such interim entries and exits: once in the second quarter of 2010, several instances in the fourth quarter of 2010, and twice in 2011.

[24] CIP-006-3c R6 has an assigned VSL of "Severe." This is considered a binary requirement, where every violation is assigned a "Severe" VSL.
[25] URE submitted a Self-Report to Reliability*First* and to SPP RE and Texas RE.

On once instance, an employee with authorized unescorted access privileges escorted a Heating, Ventilation, and Air Conditioning (HVAC) contractor into one of URE's substations. The employee called the operations center pursuant to URE's policy, but failed to inform the operations center that he was escorting a visitor into the PSP. While he was on site, the HVAC contractor entered and exited the PSP multiple times, none of which were logged because the facility did not have the capability of tracking exits electronically.

During a two-month period, URE conducted an internal audit of its visitor logging records for facilities. URE discovered several discrepancies in the logs, including illegible writing, visitors not uniquely identified, no date of entry, no date of exit, and time in logged as occurring after the time out.

During a construction project at one of its facilities, URE's construction foreman, who had authorized unescorted access privileges to a PSP, deviated from URE policy by implementing a paper logging process to avoid making numerous calls to the operations center. Although the paper logs recorded visitors' first entry and last exit from the PSP each day, it did not capture the visitors' interim entries and exits.

On once instance, an URE employee manually logged in and out two HVAC contractors as visitors. However, URE discovered in a later review of the visitor log that it did not record the HVAC contractors' interim entries and exits.

On a second instance, an URE employee with authorized unescorted access to a PSP escorted a visitor in and out of the PSP several times, but failed to notify the operations center of each visitor entry and exit, including interim entries and exits.

URE submitted a Self-Report to Reliability*First* identifying five additional instances of noncompliance with CIP-006-3c R6. These instances occurred only in the Reliability*First* region. First, a technician escorted an URE employee into one facility. The technician did not follow URE's procedures. Therefore, URE did not properly log the employee's access to the PSP.

Second, URE discovered that a member of its janitorial staff escorted, but failed to sign in, another janitorial staff member to a URE facility.

Third, the operations center received "secondary door forced open" alarms for the control building at another of URE's facilities. Shortly after the operations center received the alarms, an

URE employee called the operations center to report that the alarms occurred when he swiped his badge and opened the door. The URE employee noted that it appeared that the door was not latched all the way shut when he tried to open the door. Operations center staff checked the URE employee's access credentials and found that although he did have unescorted access privileges to other PSPs at other substations, he did not have the required access to enter the control building the facility without an escort. Operations center staff also verified that the doors were closed and secured and that the URE employee was escorted at all times.

Fourth, an URE supervisor, who had unescorted access privileges to one of URE's facilities, escorted other URE employees who did not have unescorted access privileges. The URE supervisor failed to contact the operations center to log the employees in and out, but they were escorted at all times while another facility.

Finally, an n URE technician arrived at URE's facility to assist another URE group. The technician logged the visitor entry, performed escort duties while the technician performed the work, and logged him out at the end of the day. Later that day, the technician realized that he failed to log the visitor's entry and exit with the operations center.

The Regional Entities determined that URE violated CIP-006-3c R6 for its failure to ensure that it properly logged access for all individuals twenty-four hours a day, seven days a week.

The Regional Entities determined the duration of the violations to be from the first date on which URE failed to properly log a visitor's access to the PSP, to the date URE completed its Mitigation Plan.

The Regional Entities and URE determined that these violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. NERC, based on evaluation of the facts and circumstances of this violation and similar violations from other Regional Entities, determined that this violation posed a minimal risk to the reliability of the BPS. The risk was mitigated by the fact that in all the instances, URE left no visitors unescorted, and it logged the visitors during their initial entries and final exits from the PSP.

CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379)

CIP-007-3 R8 provides, in pertinent part: "Cyber Vulnerability Assessment - The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually."

CIP-007-3 R8 has a "Lower" VRF[26] and a "Severe" VSL.[27]

URE submitted Self-Reports for CIP-007-3 R8 to the Regional Entities. URE reported that it failed to perform annual Cyber Vulnerability Assessments on certain Cyber Assets. Specifically, URE failed to perform annual Cyber Vulnerability Assessments of ports, services, or default accounts on servers where host applications are used for physical security and port scanning, to support file transfers between applications, and to provide domain authentication services.

URE also failed to perform annual Cyber Vulnerability Assessments on certain servers and workstations that are used to monitor and dispatch URE's generation fleet. URE represented that it performed initial baseline Cyber Vulnerability Assessments to use as a basis for comparison, but lacked evidence to prove that it reviewed the baseline Cyber Vulnerability Assessments annually, as required by CIP-007-3 R8.

The Regional Entities determined that URE violated CIP-007-3 R8 for its failure to perform Cyber Vulnerability Assessments of all Cyber Assets within the ESP at least annually.

The Regional Entities determined the duration of the violations to be from the date URE was required to be compliant with CIP-007-1 to the date URE completed the required Cyber Vulnerability Assessments on the affected Cyber Assets.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, although URE failed to perform annual Cyber Vulnerability Assessments, URE performed an initial, baseline Cyber Vulnerability Assessment on all affected assets. Second, URE protects against cyber attacks through multiple layers of physical and

[26] CIP-007-3 R8 and R8.1 each have a "Lower" VRF. CIP-007-3 R8.2, R8.3 and R8.4 each have a "Medium" VRF.
[27] CIP-007-3 R8 has an assigned VSL of "Severe." This is considered a binary requirement, where every violation is assigned a "Severe" VSL.

electronic security. URE has redundancy in its server and workstation environments that would require potential attackers to bypass multiple layers of control, including human observation. Third, URE performed annual Cyber Vulnerability Assessments on its other servers and workstations, and represents that these violations were isolated to one set of servers and workstations.

CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369)

CIP-004-3 R4 provides, in pertinent part:

> 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.
>
> R4.2. 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-004-3 R4 has a "Lower" VRF and a "Moderate" VSL.

URE submitted Self-Reports for CIP-004-3 R4 to the Regional Entities. URE reported that it failed to remove an IT contractor's electronic access to CCAs within seven calendar days after the IT contractor resigned from his position.

The Regional Entities determined that URE violated CIP-004-3 R4.2 for its failure to revoke access to CCAs within seven calendar days for an individual who no longer required such access to CCAs.

The Regional Entities determined the duration of the violations to be seven calendar days after the date the IT contractor resigned from URE, to the date that URE removed the IT contractor's access to CCAs.

The Regional Entities and URE determined that these violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. NERC, based on evaluation of the facts and circumstances of these violations and similar violations from other regional entities,

determined that these violations posed a minimal risk to the reliability of the BPS. Specifically, the risk to the BPS was mitigated by several factors. First, URE revoked the IT contractor's access nineteen days after he resigned and less than two weeks from the seven-day deadline imposed by CIP-004-3 R4.2. Second, the IT contractor did not have physical access to CCAs, and could not electronically access any CCAs because URE collected his network identification token, laptop, and company identification upon his resignation.

II. Violations discovered during multi-regional Compliance Audit[28]

CIP-005-3a R2 (RFC2011001078, SPP201100612, TRE201100371)

The purpose statement of Reliability Standard CIP-005-3a provides: "Standard CIP-005-3 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-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a R2 provides, in pertinent part:

> Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
> >
> > R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

[28] Reliability*First* led a Compliance Audit of URE with the participation of SPP RE and Texas RE. The Regional Entities discovered four violations of the Reliability Standards, as described below.

CIP-005-3a R2 has a "Medium" VRF[29] and a "Severe" VSL.[30]

During the Compliance Audit, URE failed to provide evidence that it enabled only ports and services required for operations and for monitoring Cyber Assets within the ESP. Although URE conducted an annual review of all ports and services, it did not maintain a baseline record of required ports and services.

URE did not conduct its annual review of ports and services using a baseline record, and therefore could not determine a history of modifications to the ports and services in order to verify their configurations. Additionally, URE did not provide a list of the ports and services and the reason that they were open. URE also failed to maintain a document identifying the content of all its required appropriate use banners.

The Regional Entities determined that URE violated CIP-005-3a R2 for its failure to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, as required by R2.2. URE also failed to maintain a document identifying the content of its appropriate use banners, as required by R2.6.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-005-1 to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS because the risk to the BPS was mitigated by several factors. First, URE represented that it performed an annual review of each Cyber Asset, and documented the process for each Cyber Asset to ensure that it enables only ports and services required for operations and monitoring of Cyber Assets within the ESP. During this annual review, URE subject matter experts looked for unneeded ports, or anomalous entries. URE documented the results of this review. Second, URE implemented appropriate use banners on all its access control devices, but failed only to document the content of all such banners.

[29] CIP-005-3a R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF. CIP-005-3a R2.5 and its subrequirements, as well as R2.6, each have a "Lower" VRF.
[30] CIP-005-3a R2 and all of its subrequirements have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.

CIP-005-3a R4 (RFC2011001079, SPP201100613, TRE201100372)

CIP-005-3a R4 provides, in pertinent part:

> 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:
>
> > R4.2. 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.

CIP-005-3a R4 has a "Medium" VRF[31] and a "Severe" VSL.[32]

At the Compliance Audit, URE failed to provide a list of ports and services that are required for operations of the electronic access points to the ESPs. URE provided documentation of an annual review of ports and services and documentation of the function for each port and service, including initial configurations, but did not provide documentation of which ports and services are required for operation, as required by CIP-005-3a R4.2.

URE also failed to discover all access points to its ESP as part of its Cyber Vulnerability Assessment, as required by CIP-005-3a R4.3. URE conducts a scan to discover all Cyber Assets connected to a network from within the ESP. While this method is effective in finding Cyber Assets within the ESP, it is not effective in determining the access points to the ESP.

The Regional Entities determined that URE violated CIP-005-3a R4 for its failure to verify that it only enabled those ports and services required for operations at access points to its ESP, as required CIP-005 R4.2, and for its failure to discover all access points to its ESP, as required by CIP-005 R4.3.

[31] CIP-005-3a R4, R4.2, R4.3, R4.4 and R4.5 each have a "Medium" VRF. CIP-005-3a R4.1 has a "Lower" VRF.
[32] CIP-005-3a R4 has an assigned VSL of "Severe." This is considered a binary requirement, where every violation is assigned a "Severe" VSL.

The Regional Entities determined the duration of the violations to be from the date URE was required to be compliant with CIP-005-1, to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, regarding CIP-005-3a R4.2, URE performs a comprehensive annual review of all devices, and documents the process with the required level of detail for each individual device, to ensure that only ports and services required for operations and monitoring of Cyber Assets within the ESP are enabled. During this annual review, URE subject matter experts seek to identify unneeded ports or anomalous entries, and URE documents the results of this review.

Second, regarding CIP-005-3a R4.3, URE conducts an annual discovery scan to identify all Cyber Assets within a specific ESP. URE compares the results of this scan to a list of known devices, and then identifies and confirms access points, as applicable. URE represents that it has properly identified all the access points to the ESP. Therefore, although URE did not conduct a scan that would discover all possible access points to its ESP, URE did conduct an annual scan that discovered all Cyber Assets connected to a network within the ESP.

CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376)

CIP-007-3 R2 provides, in pertinent part: "Ports and Services - The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled."

CIP-007-3 R2 has a "Medium" VRF and a "Severe" VSL.[33]

URE implemented a process to ensure that it enables only required ports and services, but did not include certain protocol ports in its system scans that it uses in this process.

The Regional Entities determined that URE violated CIP-007-3 R2 for its failure to ensure that URE enables only those ports and services required for normal and emergency operations.

[33] CIP-007-3 R2 and all of its subrequirements have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-007-1 to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, URE uses network security controls which analyze network traffic for known and suspect malicious activity. This system considers threats affecting ports. Second, URE's ESP firewalls are specifically configured to only allow traffic using specific protocols to enter the network. This configuration prevents unsolicited traffic from passing into the networks segregated by ESPs, thereby reducing the risk to the BPS.

CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377)

CIP-007-3 R3 provides:

> Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement 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.

CIP-007-3 R3 has a "Lower" VRF and a "Severe" VSL.[34]

[34] CIP-007-3 R3 and all of its subrequirements have an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.

During a period of about five months, URE experienced an outage of a third-party software application that included a patch management feature that URE uses to implement CIP-007 processes. During the time period that this application malfunctioned, URE failed to assess the applicability of patches for its third-party software applications. URE did not have a backup method in place for identifying or assessing security patches and upgrades. Additionally, during the Compliance Audit, an URE subject matter expert asserted that URE automatically deems all security patches to be applicable and therefore did not maintain documentation of the assessment of security patches and upgrades for applicability.

The Regional Entities determined that URE violated CIP-007-3 R3 for its failure to document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades, as required by R3.1, and for its failure to document the implementation of security patches, as required by R3.2.

The Regional Entities determined the duration of the violations to be from the date on which URE was required to be compliant with CIP-007-1 to the date URE completed its Mitigation Plan.

The Regional Entities determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was mitigated by several factors. First, URE represented that it had installed all applicable security patches, although it did not document this policy in URE's patch management program. Second, URE was applying "defense-in-depth" strategies. Third, URE protects the systems in question by requiring authentication, which also employs antivirus protection and host intrusion prevention software.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, the Regional Entities had assessed a penalty of ninety thousand dollars ($90,000) for the referenced violations. In reaching this determination, the Regional Entities considered the following factors:

1. The Regional Entities considered certain aspects of URE's internal compliance program (ICP) as a mitigating factor in the penalty determination;
2. The Regional Entities also considered that URE self-reported some of the violations;
3. The Regional Entities considered URE's violation history as an aggravating factor in the penalty determination;

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

After consideration of the above factors, the Regional Entities determined that, in this instance, the penalty amount of ninety thousand dollars ($90,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[35,36]

I. Self-Reported Violations

CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205)

URE's first Mitigation Plan to address its violation of CIP-007-3 R5was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for this violation is designated as MIT-10-3341 and was submitted as non-public information to FERC in accordance with FERC orders.[37]

URE's Mitigation Plan required URE to:

1. Modify the password to meet as many CIP requirements as technically feasible;

[35] *See* 18 C.F.R § 39.7(d)(7).
[36] The Mitigation Plans listed below apply to the violations identified in the three regions involved. The Regional Entities' decision to coordinate their enforcement actions took place after the Mitigation Plans were submitted to FERC.
[37] A Mitigation Plan designated as MIT-08-3487 and addressing SPP201000447 was submitted to FERC. However, this Mitigation Plan was submitted before the Regional Entities coordinated their enforcement actions and determined that Reliability*First* would take the lead in enforcing the Standards involved. As a result, the Mitigation Plan was replaced by the Mitigation Plan described in this Full Notice of Penalty and in the Settlement Agreement.

2. File a Technical Feasibility Exception (TFE) if needed;
3. Correct all account passwords by either removing the account or ensuring that the users changed their passwords; and
4. Perform a system impact assessment and develop related procedures, forms and tools to prevent recurrence of this violation.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

URE's second Mitigation Plan to address its violation of CIP-007-3 R5 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT005761 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete the reviews of local accounts on the Cyber Assets at issue;
2. Review and update management controls to improve methods used to communicate and monitor the annual reviews for local user accounts; and
3. Communicate the process changes to relevant URE personnel.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of the Mitigation Plan. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

URE submitted a third Mitigation Plan for CIP-007-3 R5[38] subsequent to the discovery of an additional possible violation. Upon further review, Reliability*First* dismissed the new possible violation as it represented an expansion in scope of the original. Reliability*First* treated this

[38] This Mitigation Plan addressed the violation discovered during the multi-regional Compliance Audit and incorrectly references to RFC2011001083.

Mitigation Plan as a modification of URE's previously approved Mitigation Plan.. The additional milestones extended to the approved completion date.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's modified Mitigation Plan was completed.

URE's Mitigation Plan required URE to form a cross functional team of subject matter experts to perform a comprehensive review and analysis of the audit findings. This team would establish and implement a process to document all shared application and database used accounts, and to account for and log all individual user activity.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291)

URE's Mitigation Plan to address its violations of CIP-007-1 R6 was submitted to Reliability*First.* The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005462 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review and update its existing process and procedure documents;
2. Enable alerting on all of the Cyber Assets that were reporting logs into the log management system;
3. Remediate all remaining Cyber Assets not reporting their logs into the log management system; and
4. Enable all alerting on the remaining Cyber Assets.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368)

URE's Mitigation Plan to address its violations of CIP-004-3 R3 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005894 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review all background checks for affected personnel;
2. Order and complete new background checks when needed; and
3. Modify URE's software program that processes inbound background check data to ensure that it completes all background check elements for a PRA.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373)

URE's first Mitigation Plan to address its violation of CIP-006-3c R1was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT005467 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Remove the Cyber Assets from the ESP;
2. Disable the ESP connection point; and

3. Implement management controls to ensure that new Cyber Assets are located within the PSP.

URE certified in a document submitted to Reliability*First* that the above Mitigation Plan requirements were completed and submitted evidence of completion.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

URE's second Mitigation Plan to address its violation of CIP-006-3c R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT005763 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Repair the malfunctioning strike plate; and
2. Conduct a CIP training meeting to review visitor escorting policies and procedures.

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

On after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

URE's third Mitigation Plan to address its violation of CIP-006-3c R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT005467 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Evaluate multiple Mitigation Plan options for feasibility;

2. Evaluate the operational impact of any changes. These changes include system updates, hardware installation, and staff training; and
3. Implement the approved changes.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374)

URE's Mitigation Plan to address its violations of CIP-006-3c R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005912 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Enable alerting on affected firewalls;
2. Review relevant process documents and identify required changes; and
3. Revise its CIP-005 R3.2 document to include the firewalls at issue.

URE certified in a document submitted to Reliability*First* that the above Mitigation Plan requirements were completed and submitted evidence of completion.

After reviewing of URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375)

URE's Mitigation Plan to address its violations of CIP-006-3c R6 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005888 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Modify URE's operations center script to emphasize the need for employee escorts to report each visitor's entry and exit;
2. Modify URE's issues management process to include supervision of personnel involved in logging incidents;
3. Create and deliver a presentation to employees about the proper methods for visitor logging;
4. Increase the use of operations center logging – convert from use of manual logging to calling the operations center to ensure that logging is complete and accurate;
5. Disseminate the presentation about the proper methods for visitor logging to all personnel with authorized unescorted access to CCAs across the company;
6. Develop standardized paper log sheets; and
7. Enhance URE's annual CIP web-based training to focus on issues regarding visitor logging.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379)

URE's Mitigation Plan to address its violations of CIP-007-3 R8 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as MIT-09-3846 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review its existing management controls to identify potential improvements in the processes governing the Cyber Vulnerability Assessment process and associated documentation required for evidence of compliance;
2. Implement improvements to the Cyber Vulnerability Assessment processes; and

3. Communicate process changes and evidence requirements to the appropriate personnel.

URE certified in a document submitted to Reliability*First* that the above Mitigation Plan requirements were completed and submitted evidence of completion.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369)

URE's Mitigation Plan to address its violations of CIP-004-3 R4 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT005889 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Remove the IT contractor's access to the CCAs;
2. Issue a communication to all IT managers with employees or contractors who have NERC CIP electronic or unescorted physical access privileges related to:
    a. CIP Standards regarding access termination;
    b. The URE process for terminating individuals with access; and
    c. The importance of the urgency to revoke access.
3. Issue quarterly manager reminders related to the managers' responsibilities for managing access termination of employees or contractors with CIP access.

URE certified in a document submitted to Reliability*First* that the above Mitigation Plan requirements were completed and submitted evidence of completion.

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

II. Violations discovered during the multi-regional Compliance Audit

CIP-005-3a R2 (RFC2011001078, SPP201100612, TRE201100371);
CIP-005-3a R4 (RFC2011001079, SPP201100613, TRE201100372); and
CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376)

URE's Mitigation Plan to address its violations of CIP-005-3a R2, CIP-005-3a R4 and CIP-007-3 R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006044 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Perform a comprehensive review and analysis of the audit findings and evaluate multiple options for modifying processes and creating additional documentation to demonstrate compliance;
2. Regarding ports and services:
    a. Perform a preliminary identification of ports and services collection methods;
    b. Draft format for ports and services configuration baseline;
    c. Catalog the ports, document the business use for each port, establish baseline of ports for each device type, and use the baseline to identify anomalies in the current configuration of each device;
    d. Identify and describe tool-based technical solutions for consideration; and
    e. Issue a recommendation for approval;
3. Regarding banners:
    a. Document the approved banner for administrative access to the ESP access points;
    b. Determine which interfaces on which access points can support the banner;
    c. Determine which interfaces cannot support the banner and require a TFE;
    d. Submit TFEs if needed; and
    e. Configure the banner on all administrative interfaces on all ESP access points;
4. Regarding ESP access points:
    f. Identify and document which ESP devices are in scope for remediation;
    g. Identify multiple tool-based technical options for identifying all possible access points to the ESP; and
    h. Recommend changes for approval;

5. Design a plan to implement remedial actions for ports and services, ESP access points and banners across; and
6. Implement the approved actions in three phases.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377)

URE's Mitigation Plan to address its violations of CIP-007-3 R3 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* on behalf of the Regional Entities on and approved by NERC. The Mitigation Plan for these violations is designated as RFCMIT006046 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review its security patch management practices;
2. Identify an appropriate mechanism for assessing security patches for applicability;
3. Document backup assessment procedures;
4. Update its procedures and supporting documentation; and
5. Deploy the new practices.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[39]

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,[40] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2012. The NERC BOTCC approved the Settlement Agreement, including the Region's assessment of a ninety thousand dollar ($90,000) 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. The Regional Entities considered certain aspects of URE's ICP as a mitigating factor in the penalty determination;
2. The Regional Entities also considered that URE self-reported some of the violations;
3. The Regional Entities considered URE's violation history as an aggravating factor in the penalty determination;
4. The Regional Entities reported that URE was cooperative throughout the compliance enforcement process;
5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. The Regional Entities determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. The Regional Entities reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[39] *See* 18 C.F.R. § 39.7(d)(4).
[40] *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).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of ninety thousand dollars ($90,000) 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.

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 the Regional Entities and URE executed March 30, 2012, included as Attachment a;

    1. URE's Self-Reports for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment A to the Settlement Agreement;
    2. URE's Self-Reports for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment B to the Settlement Agreement;
    3. URE's Mitigation Plan for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment C to the Settlement Agreement;
    4. URE's Certification of Mitigation Plan Completion for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment D to the Settlement Agreement;
    5. The Regional Entities' Verification of Mitigation Plan Completion for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment E to the Settlement Agreement;
    6. URE's Mitigation Plan for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment F to the Settlement Agreement;
    7. URE's Certification of Mitigation Plan Completion for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205) submitted to Reliability*First*, included as Attachment G to the Settlement Agreement;

8. URE's Mitigation Plan for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment H to the Settlement Agreement;
9. URE's Self-Reports for CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291), included as Attachment I to the Settlement Agreement;
10. URE's Mitigation Plan for CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291), included as Attachment J to the Settlement Agreement;
11. URE's Self-Report for CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368), included as Attachment K to the Settlement Agreement;
12. URE's Mitigation Plan for CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368), included as Attachment L to the Settlement Agreement;
13. URE's Certification of Mitigation Plan Completion for CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368), included as Attachment M to the Settlement Agreement;
14. URE's Self-Reports for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment N to the Settlement Agreement;
15. URE's Self-Reports for CIP-006-3c R1 (RFC201100933, SPP201100589), included as Attachment O to the Settlement Agreement;
16. URE's Mitigation Plan for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment P to the Settlement Agreement;
17. URE's Certification of Mitigation Plan Completion for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment Q to the Settlement Agreement;
18. URE's Mitigation Plan for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment R to the Settlement Agreement;
19. URE's Certification of Mitigation Plan Completion for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment S to the Settlement Agreement;
20. URE's Mitigation Plan for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment T to the Settlement Agreement;
21. URE's Self-Reports for CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374), included as Attachment U to the Settlement Agreement;

22. URE's Mitigation Plan for CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374), included as Attachment V to the Settlement Agreement;
23. URE's Certification of Mitigation Plan Completion for CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374), included as Attachment W to the Settlement Agreement;
24. The Regional Entities' Verification of Mitigation Plan Completion for CIP-006-3c R2 (RFC201100934, SPP201100588, TRE201100374), included as Attachment X to the Settlement Agreement;
25. URE's Self-Reports for CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375), included as Attachment Y to the Settlement Agreement;
26. URE's Mitigation Plan for CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375), included as Attachment Z to the Settlement Agreement;
27. URE's Certification of Mitigation Plan Completion for CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375), included as Attachment AA to the Settlement Agreement;
28. URE's Self-Reports for CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379), included as Attachment BB to the Settlement Agreement;
29. URE's Mitigation Plan for CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379), included as Attachment CC to the Settlement Agreement;
30. URE's Certification of Mitigation Plan Completion for CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379), included as Attachment DD to the Settlement Agreement;
31. URE's Self-Reports for CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369), included as Attachment EE to the Settlement Agreement;
32. URE's Mitigation Plan for CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369), included as Attachment FF to the Settlement Agreement;
33. URE's Certification of Mitigation Plan Completion for CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369), included as Attachment GG to the Settlement Agreement;

34. The Regional Entities' Verification of Mitigation Plan Completion for CIP-004-3 R4 (RFC201100948, SPP201100594, TRE201100369), included as Attachment HH to the Settlement Agreement;

35. URE's Mitigation Plan for CIP-005-3 R2 (RFC2011001078, SPP201100612, TRE201100371), included as Attachment II to the Settlement Agreement;

36. URE's Mitigation Plan for CIP-005-3 R4 (RFC2011001079, SPP201100613, TRE201100372), included as Attachment JJ to the Settlement Agreement;

37. URE's Mitigation Plan for CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376), included as Attachment KK to the Settlement Agreement; and

38. URE's Mitigation Plan for CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377), included as Attachment LL to the Settlement Agreement.

b) URE's Certifications of Mitigation Plan Completion for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment b;

c) The Regional Entities' Verifications of Mitigation Plan Completion for CIP-007-3 R5 (RFC201000690, SPP201000447, TRE201000205), included as Attachment c;

d) URE's Certification of Mitigation Plan Completion for CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291), included as Attachment d;

e) The Regional Entities' Verification of Mitigation Plan Completion for CIP-007-3 R6 (RFC201100769, SPP201100518, TRE201100291), included as Attachment e;

f) The Regional Entities' Verification of Mitigation Plan Completion for CIP-004-3 R3 (RFC201100931, SPP201100586, TRE201100368), included as Attachment f;

g) URE's Certifications of Mitigation Plan Completion for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment g;

h) The Regional Entities' Verifications of Mitigation Plan Completion for CIP-006-3c R1 (RFC201100933, SPP201100589, TRE201100373), included as Attachment h;

i) The Regional Entities' Verification of Mitigation Plan Completion for CIP-006-3c R6 (RFC201100935, SPP201100595, TRE201100375), included as Attachment i;

j) The Regional Entities' Verification of Mitigation Plan Completion for CIP-007-3 R8 (RFC201100936, SPP201100591, TRE201100379), included as Attachment j;

k) The Regional Entities' Source Document for CIP-005-3a R2 (RFC2011001078, SPP201100612, TRE201100371), CIP-005-3a R4 (RFC2011001079, SPP201100613, TRE201100372), CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376) and CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377) not dated, included as Attachment k;

l) URE's Certifications of Mitigation Plan Completion for CIP-005-3a R2 (RFC2011001078, SPP201100612, TRE201100371), CIP-005-3a R4 (RFC2011001079, SPP201100613, TRE201100372) and CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376), included as Attachment l;

m) The Regional Entities' Verification of Mitigation Plan Completion for CIP-005-3a R2 (RFC2011001078, SPP201100612, TRE201100371), CIP-005-3a R4 (RFC2011001079, SPP201100613, TRE201100372) and CIP-007-3 R2 (RFC2011001081, SPP201100615, TRE201100376), included as Attachment m;

n) URE's Certifications of Mitigation Plan Completion for CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377), included as Attachment n; and

o) The Regional Entities' Verification of Mitigation Plan Completion for CIP-007-3 R3 (RFC2011001082, SPP201100616, TRE201100377), included as Attachment o.

A Form of Notice Suitable for Publication[41]

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

[41] *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 charles.berardesco@nerc.net Robert K. Wargo* Director of Analytics & Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org L. Jason Blake* General Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 jason.blake@rfirst.org	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Meredith May Jolivert* Attorney North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005-3801 (202) 644-8052 (202) 644-8099 – facsimile rebecca.michael@nerc.net meredith.jolivert@nerc.net Susan Vincent* General Counsel Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4922 (512) 233-2233 – facsimile susan.vincent@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

Megan E. Gambrel* Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 megan.gambrel@rfirst.org Michael D. Austin* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 mike.austin@rfirst.org *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.	Ron Ciesiel* General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 614-3265 (501) 482-2025 – facsimile rciesiel.re@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1672 (501) 482-2025 – facsimile Jgertsch.re@spp.org Peggy Lewandoski* Paralegal & SPP RE File Clerk Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 482-2057 (501) 482-2025 – facsimile Spprefileclerk.re@spp.org

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Meredith May Jolivert
Attorney
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
meredith.jolivert@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation, Southwest Power Pool Regional Entity and Texas Reliability Entity, Inc.

Attachments