PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

October 30, 2014

VIA ELECTRONIC FILING

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. NP15-_-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# NCRXXXXXX, 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] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred and six thousand dollars ($106,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[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 (2014). *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) and 18 C.F.R § 39.7(d).

[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.

conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty 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, 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 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012232	CIP-002-1	R2	High/Severe	$106,000
TRE2013012261	CIP-002-1	R3; R3.1; R3.2	High/Severe	
TRE2013012233	CIP-003-1	R4; R4.3	Medium/Severe	
TRE2012011153	CIP-003-1	R5; R5.1; R5.2; R5.3	Lower/Severe	
TRE2012011159	CIP-004-1	R4; R4.1	Lower/Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012235	CIP-005-1	R1; R1.4; R1.6	Medium/ Moderate	$106,000
TRE2012011177	CIP-005-3	R5; R5.2	Lower/Lower	
TRE2013012262	CIP-006-1	R3	Medium/ Moderate	
TRE2013012624	CIP-006-3c	R5	Medium/Severe	
TRE2013012625	CIP-006-3c	R6	Lower/Severe	
TRE2012011178	CIP-007-1	R1; R1.1; R1.2; R1.3	Medium/High	
TRE2013012970	CIP-007-3a	R1; R1.2; R1.3	Medium/Severe	
TRE2013012968	CIP-007-1	R2; R2.1	Medium/Severe	
TRE2012011179	CIP-007-3a	R3; R3.1; R3.2	Lower/Severe	

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012971	CIP-007-3a	R3; R3.2	Lower/Severe	$106,000
TRE2012010877	CIP-007-1	R4	Medium/Moderate	
TRE2013012972	CIP-007-3a	R4; R4.2	Medium/Severe	
TRE2013012234	CIP-007-1	R5; R5.1; R5.2; R5.3.3	Medium/Severe	
TRE2012011180	CIP-007-2a	R9	Lower/High	
TRE2012011181	CIP-008-3	R1; R1.2	Lower/Moderate	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

OVERVIEW

This Settlement Agreement resolves 20 CIP violations discovered throughout 2012 and 2013. The violations were discovered through a series of Self-Certifications, Self-Reports, and a Compliance Audit.

CIP-002-1 R2 (TRE2013012232)

URE submitted a Self-Report stating that it was in violation of CIP-002-1 R2. Specifically, URE reported that it discovered errors in its list of identified Critical Assets determined through an annual application of its risk-based assessment methodology. URE discovered that, in several instances, it erroneously included or omitted substations on its Critical Assets list. The cause was an oversight by URE when transcribing Critical Asset information from its various maps and lists to the final Critical Assets list.

Texas RE determined that URE had a violation of CIP-002-1 R2 for failing to update its Critical Asset lists accurately after applying its annual risk-based assessment methodology.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed preparation of its Critical Assets list.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE applied its annual risk-based assessment methodology. Although URE did not include certain Critical Assets on its official Critical Assets list, URE correctly identified its Critical Assets on maps and other lists as Critical Assets and protected them as such. URE managed all station-based Cyber Assets with the same safeguards, using the same procedures, processes, security measures, tools, and protocols.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. finalize its new procedure containing its methodology for identifying Critical Assets and updating CCAs and Technical Feasibility Exceptions (TFEs);
2. conduct training on the new procedure for all stakeholders involved in the annual risk-based assessment process;
3. post the new procedure to its compliance database to facilitate access by appropriate personnel, and send an email to affected personnel in charge of implementing the new procedure; and
4. complete development of the annual Critical Asset list applying the new procedure.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-002-1 R3 (R3.1, R3.2) (TRE2013012261)

URE submitted a Self-Report stating that it was in violation of CIP-002-1 R3. Specifically, URE reported that it discovered errors in its CCA lists for several years. These errors consisted of the following: (i) failure to identify switches with routable protocols that were connected to two backup inter-control center protocol (ICCP) devices as CCAs (this occurred after an Electronic Security Perimeter (ESP)

reconfiguration was completed); (ii) multiple instances where stations and their associated CCAs were incorrectly included on the CCA list; and (iii) multiple instances where stations and their associated CCAs were omitted from the CCA list.

Texas RE determined that URE had a violation of CIP-002-1 R3 for failing to develop a complete and accurate list of associated CCAs essential to the operation of Critical Assets.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed development of the annual CCA list.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to document the list accurately, the CCAs that were left off the CCA list were within secured ESPs and afforded the protections included in CIP-003-1 through CIP-009-1. The CCAs were protected by URE's firewalls and by URE's intrusion prevention system. This system monitored and provided alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and investigated. URE's core network, which included all primary CCAs, was physically located in a secure room within a secure facility that was monitored at all times. Additionally, URE managed all relevant Cyber Assets with the same safeguards, procedures, processes, security measures, tools, and protocols.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. disconnect the switches and logically reconfigure them back to their original location;
2. update the CCA and ESP lists to reflect the current ESP configuration;
3. implement enhancements to the change management procedure to minimize the potential for recurrence;
4. conduct a thorough review of the devices to ensure all relevant CCAs have been identified and documented on the CCA and ESP lists. URE also developed a new procedure to document the process of completing this review on a periodic basis to ensure the ESP list is accurate;
5. train the appropriate personnel on the enhanced change management procedure and on the new procedure for establishing and maintaining ESPs;
6. implement these new procedures and post them to its compliance database to facilitate access by appropriate personnel;

7. create a new methodology for identifying CAs and updated CCAs and TFEs to include a more robust process of inclusion, reviews, and controls to help ensure accuracy of its CCA list;
8. conduct training on this new methodology with all stakeholders involved in the annual risk-based assessment process;
9. implement this new methodology and post it to its compliance database to facilitate access by appropriate personnel; and
10. complete development of the annual CCA list using the new methodology.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R4 (R4.3) (TRE2013012233)

URE submitted a Self-Report to Texas RE stating that it was in violation of CIP-003 R4. URE failed to conduct and document all annual assessments of its adherence to its CCA information protection program for two years. Specifically, URE conducted annual adherence assessments for information related to one group, but it did not document the assessments. URE failed to conduct annual adherence assessments for information related to a different URE group.

Texas RE determined that URE had a violation of CIP-003-1 R4 for failing to conduct and document all annual assessments of its adherence to its CCA protection program.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its review of its information protection program, implemented enhancements, and posted the new program documents to a location accessible by appropriate personnel.

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by failing to conduct certain annual adherence assessments of its information protection program, URE failed to have sufficient security management controls in place, and sensitive information related to CCAs could have been compromised. However, although URE did not properly document all aspects of two annual assessments, URE did control access to certain protected information and conducted reviews accordingly. Further, URE's data custodians were appropriately controlling access to documents protected under URE's information protection program.

URE's Mitigation Plan (TREMIT009150) to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a thorough evaluation of its information protection program and create an action plan to identify enhancements;
2. enhance its program documents to clarify and reinforce the requirements related to CIP-003;
3. complete training on the enhanced program documents with personnel responsible for managing protected information; and
4. implement the enhanced program and post associated documents to its compliance database to facilitate access by appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R5 (R5.1, R5.2, R5.3) (TRE2012011153)

URE submitted a Self-Certification stating that it was in violation of CIP-003-1 R5. URE subsequently submitted a more detailed Self-Report.

URE stated that it did not timely update the personnel list for those responsible for authorizing access to protected CCA information. Specifically, URE failed to remove a former employee who left the company from its data custodian list. In addition, URE did not conduct an annual review of access privileges to a particular document management site to confirm that access privileges were correct and that they corresponded with URE's needs and appropriate personnel roles and responsibilities. Moreover, URE did not at least annually assess and document the processes for controlling access privileges to protected information on that same site. URE also reported that it discovered several instances where documents designated as confidential or restricted were attached as documentation from URE's change management system. As a result, any URE or contractor employee who had access to the system could view those documents.

Texas RE determined that URE had a violation of CIP-003-1 R5 for failing to document and implement a program for managing access to protected CCA information that met the requirements of the Standard.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the date URE conducted an annual review of its processes for controlling access privileges to protected information.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/Physical Security Perimeter (PSP) access authentication.

With respect to the document management site, URE confirmed that the site had the appropriate site and document level controls and was managed to ensure controlled access to protected information.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. revise its information protection program to reflect the appropriate data custodians, post the program to its compliance database to facilitate access by appropriate personnel, and send an email communication to applicable personnel informing them that the revised program was implemented and in effect;
2. assign a new data custodian to the document management site, who implemented a process to conduct quarterly reviews of the access privileges to the site;
3. conduct training on the requirements of the revised program with all data custodians and conduct an annual review;
4. redesign the change management system to ensure only those individuals with approved access privileges to protected information can access/view change requests that include protected information;
5. conduct an end-to-end review of the program to identify opportunities and implement enhancements;
6. develop and implement processes for annual program adherence assessment;
7. design and implement an enhanced periodic access review process with centralized documentation maintained in the compliance database;

8. document access privileges criteria and processes for the document management platform, the change management system, the password site, the engineering project software, and the compliance database;
9. enhance the annual review meeting conducted with all data custodians;
10. establish periodic operational and corporate level controls to ensure implementation and adherence to the program; and
11. develop a cross-functional training program, training materials, and schedule required to implement the enhanced process and procedure improvements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (TRE2012011159)

URE submitted a Self-Certification stating that it was in violation of CIP-004-1 R4. URE subsequently submitted a more detailed Self-Report. For CCAs administered by one URE team, URE reviewed a list of personnel who had access to an application that is run on most CCAs, instead of reviewing a list of personnel who had access to the CCAs themselves.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the date URE amended its documentation to correct annual review processes and performed a review to verify the documentation changes.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, intrusion prevention, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/PSP access authentication.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a thorough review of cyber access rights for each individual account on the CCAs in the ESPs administered by the relevant team and update the access authorization list to reflect the current state of CCA access;

2. develop and implement a new process for tracking and reviewing individual account access on CCAs;
3. conduct quarterly reviews of cyber access rights of each user account on each CCA in the ESPs administered by the relevant team and make timely access adjustments;
4. continue access review and associated access adjustments based on daily URE personnel employment status change reports, including review of access for personnel with cyber access to individual accounts on CCAs in the ESPs administered by the relevant team;
5. continue access review and associated access adjustments based on proactive monitoring and communication of contract services personnel employment status, including review of access for personnel with cyber access to individual accounts on CCAs in the ESPs administered by the relevant team;
6. document formally and communicate the new process to affected employees and post the new process and procedure; and
7. identify and train the URE employees within the relevant team who will act as primary and secondary backups for the access review process.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R1 (R1.4, R1.6) (TRE2013012235)

URE submitted a Self-Report stating that it was in violation of CIP-005 R1. URE did not appropriately identify and document five non-critical Cyber Assets in the ESP. Specifically, URE failed to include on an ESP list two non-critical Cyber Assets that connected to two devices within the ESP. URE failed to include one server on any of the ESP lists generated for a period of approximately two years. Lastly, URE listed two servers as CCAs on an ESP list that was generated on a certain date, but it failed to include the servers on any subsequent lists until almost a year later.

Texas RE determined that URE had a violation of CIP-005-1 R1 for failing to identify and document five non-critical Cyber Assets in the ESP.

Texas RE determined the duration of the violation to be from the date one of the servers was not included on the ESP list through when URE updated the ESP documentation to reflect the presence of the non-critical Cyber Assets within the ESP.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it failed to include the five devices on its ESP lists, URE provided the required protections to the devices. The servers should have been classified as non-critical Cyber Assets, as they had never been moved from testing into full production. Lastly, the devices represented less than 5% of all devices protected within ESPs.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. install a network scanning tool that enables URE to conduct total system scans to monitor all ports and devices;
2. complete its new procedure to institute more stringent controls and reviews on URE's ESPs and documentation processes;
3. train the relevant team on the new procedure;
4. perform a scan of the complete ESP;
5. update ESP documentation to reflect the presence of non-critical Cyber Assets; and
6. post and implement the new procedure.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-005-3 R5 (R5.2) (TRE2012011177)

URE submitted a Self-Certification stating that it was in violation of CIP-005-3 R5. URE subsequently submitted a more detailed Self-Report.

URE reported that it failed to update documentation to reflect the modification of the network or controls within 90 calendar days of the change. Specifically, URE moved two Critical Assets from one ESP to another ESP and failed to document the change within 90 days. Further, when URE created the new documentation, it contained errors.

Texas RE determined that URE had a violation of CIP-005-3 R5 for failing to update the documentation to reflect the modification of the network or controls within 90 calendar days.

Texas RE determined the duration of the violation to be from 90 days after when URE moved the two Critical Assets from one ESP to another ESP through when URE updated its documentation to reflect the correct location of the Critical Assets.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The Critical Assets at issue were protected by URE's ESPs, and they comprised a small percentage of URE's total Critical Assets. Further, URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. Lastly, the affected devices were physically located in a secure room within a secure facility that was monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. relocate the devices from the new ESP back to the original ESP;
2. update the ESP and CCA documentation;
3. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of the violation and develop other related improvements;
4. develop and document a procedure for establishing, reviewing, and updating ESPs;
5. enhance the procedure for identifying, reviewing, and updating CCAs; and
6. develop a cross-functional training program, training materials, and schedule required to implement the enhanced process and procedure improvements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R3 (TRE2013012262)

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R3. Specifically, although appropriately equipped with card reader access restrictions managed through URE's access management and logging system, URE was not monitoring access to one of its PSP doors. The door

was left off the list for URE's security management contractor. Because the door was not being monitored by the security contractor, URE was not immediately reviewing unauthorized access attempts to a PSP for the door.

Texas RE determined that URE had a violation of CIP-006-1 R3 for failing to implement technical and procedural controls for monitoring physical access at all access points to the PSP at all times.

Texas RE determined the duration of the violation to be from the date the standard became mandatory and enforceable on URE through the date URE transferred access monitoring from the contractor to URE.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The door was located in a secure URE facility that was staffed at all times. Further, the door was appropriately equipped with card reader access restrictions managed through URE's access management and logging system.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. enhance its physical security plan based on results of URE's annual procedure review;
2. update the plan to reflect the current security measures as observed through a walk-through of the PSP;
3. provide training to appropriate personnel on the enhanced plan;
4. post and implement the enhanced plan; and
5. bring PSP access monitoring fully under URE's supervision.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R5 (TRE2013012624)

URE submitted a Self-Report stating that it was in violation of CIP-006-3c R5. URE explained that it replaced an existing air conditioning unit in service in a PSP. A panel was removed from the wall of the PSP and from the wall of the adjacent mechanical room to provide venting for the temporary air

conditioning unit. The removal of those panels created a space in the wall, thereby creating a temporary access point to the PSP. Security monitoring equipment was in place and was monitoring and logging access to the temporary access point. However, alarming had been disabled.

Several hours later, a URE employee investigated and determined that alarming was not in place for the temporary access point, and requested that it be re-initiated. Alarming was re-initiated a few minutes later.

Texas RE determined that URE had a violation of CIP-006-3c R5 for failing to implement its technical and procedural controls for monitoring physical access at all access points to the PSP at all times.

Texas RE determined the duration of the violation to be for several hours, from the time the temporary access point was created until alarming was re-initiated.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The temporary access point was located within a secured and monitored building protected by a secured, fenced yard. Both the building and the yard were equipped with key card access control, and the area was staffed at all times. Security monitoring equipment was in place and was monitoring and logging access to the temporary access point. However, the alarming was off for the period of the violation. Logging of the temporary access point indicated that there was no activity in the mechanical room within the period that alarming was disabled.

URE's Mitigation Plan to address this violation was submitted to Texas RE.

URE's Mitigation Plan required URE to:

1. re-initiate alarming for the temporary access point;
2. install permanent grating over the penetration in the PSP to eliminate the possibility of recurrence; and
3. distribute, to managers and supervisors at the PSP, URE's procedure specifying the controls used to manage access to PSPs.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R6 (TRE2013012625)

URE submitted a Self-Report to Texas RE stating that it was in violation of CIP-006-3c R6. URE failed to ensure that an air conditioning contractor working in a PSP signed URE's access log as required by URE's physical security plan. The contractor was appropriately escorted during his presence in the PSP.

Texas RE determined that URE had a violation of CIP-006-3c R6 for failing to implement its technical and procedural mechanisms for logging physical entry at all access points to the PSP.

Texas RE determined the duration of the violation to be for several hours on the date the contractor worked in the PSP without having signed the access log.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The contractor was appropriately escorted at all times while inside the PSP. Further, the PSP was within a secured and monitored building that was within a secured, fenced yard. Both the building and the yard were equipped with key card access control, and the area was staffed at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE.

URE's Mitigation Plan required URE to:

1. provide specific counseling relating to CIP physical security requirements and URE's physical security plan to the employee who escorted the contractor within the PSP but failed to ensure the contractor signed the access log;
2. reinforce the applicable requirements related to CIP physical security and URE's physical security plan with each member of staff leadership at the PSP, including all managers and supervisors; and
3. require its managers and supervisors at the PSP to review and acknowledge the procedure that specifies the controls used to manage access to PSPs.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (R1.1, R1.2, R1.3) (TRE2012011178)

URE submitted a Self-Certification stating that it was in violation of CIP-007-1 R1. URE subsequently submitted a more detailed Self-Report. URE reported that it failed to complete documentation that it performed testing, prior to making changes to existing Cyber Assets, in a manner that reflects the production environment. URE also reported that it failed to implement its procedure effectively to ensure personnel understood the need to document that testing was performed in a manner that reflects the production environment and to document test results in URE's change management system.

Texas RE determined that URE had a violation of CIP-007-1 R1 for failing to implement effectively its test procedures to ensure that changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

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

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE did not properly train its personnel. Failure to document that significant changes to the Cyber Assets within the ESP were tested in a manner that reflects the production environment and to document test results could have introduced vulnerabilities or modified existing cybersecurity controls. However, although not consistently documented, significant changes to Cyber Assets within the ESP were tested in a manner that reflects the production environment. All CCAs were protected by URE's firewalls and its intrusion prevention system, which was monitoring and providing alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and investigated. Further, URE's primary CCAs were physically located in a secure room within a secure URE facility that is monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a review of URE's change management procedure and make enhancements to the testing plan included in the procedure;
2. conduct training on the enhanced procedure for the members of the team who perform testing of changes to Cyber Assets within the ESPs that they administer. The training was designed to ensure that personnel understand the need to document that testing is performed in a manner

that reflects the production environment and that all test results must be documented in URE's change management system;

3. implement and post the updated procedure to a database to facilitate access by relevant personnel; and
4. establish a team to address the causes of this violation and to develop other related process improvements, as appropriate.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-3a R1 (R1.2, R1.3) (TRE2013012970)

During the Compliance Audit, Texas RE determined that URE was in violation of CIP-007-3a R1. URE did not document the test results for a number of change requests for significant changes as required by URE's change control and configuration management procedure. Texas RE determined certain change requests for significant changes to Cyber Assets within an ESP did not contain evidence indicating testing processes were followed or testing results were documented as required by that procedure.

Texas RE determined that URE had a violation of CIP-007-3a R1 for failing to document that testing is performed in a manner that reflects the production environment and for failing to document test results.

Texas RE determined the duration of the violation to be from the date documentation was discovered missing through when URE amended its procedure to provide more clarity on the necessary steps for testing and documentation.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did document change requests completed for significant changes to Cyber Assets within ESPs, but did not retain documentation related to testing processes and results prior to the change requests being completed. Further, testing of significant changes is done within URE's development environment and prior to application within ESPs.

To mitigate this violation, URE:[4]

1. conducted training on the change management test plan;

[4] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012970.

2. updated its process to provide more clarity on the necessary steps for testing and documentation, and created a change approval board as a new control to manage and monitor the completion and documentation of changes;
3. reviewed results of the Compliance Audit and reinforced focus on compliance in meeting of the relevant URE team;
4. added information technology operational expertise to the relevant URE team as part of a phased approach to organizational realignment;
5. developed change request documentation guide providing more clarity on impact assessment, work plan, test plan, and test results documentation;
6. established and implemented enhanced change request approval and review processes;
7. reviewed all open change requests for required documentation prior to close-out for significant changes implemented after a certain date;
8. enhanced URE's change management and responsibilities matrix procedures to clarify individual expectations and accountabilities;
9. trained relevant personnel on procedural enhancements; and
10. implemented and posted enhanced procedures.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R2 (R2.1) (TRE2013012968)

During the Compliance Audit, Texas RE discovered that URE failed to disable ports and services that were not required for normal and emergency operations. Texas RE enforcement determined that URE opened two ports and services on a single device to support troubleshooting and testing, but it inadvertently failed to turn them off when introducing the device to the production environment.

Texas RE determined that URE had a violation of CIP-007-1 R2 for failing to implement its process to ensure that only those ports and services required for normal and emergency operations are enabled.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE removed the ports and services.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The ports at issue were not required for normal or emergency operations but

were enabled for testing purposes. The ports represented point-to-point connections between Cyber Assets, and other Cyber Assets outside the specific environment could not access them.

To mitigate this violation, URE:[5]

1. removed the ports and services that were inadvertently left open; and
2. strengthened its approach to preparing devices to enter the production environment.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-3a R3 (R3.1, R3.2) (TRE2012011179)

URE submitted a Self-Certification stating that it was in violation of CIP-007-3a R3. URE subsequently submitted a more detailed Self-Report. URE stated that, in two instances, it failed to assess, and therefore document, security patches for two types of servers.

Texas RE determined that URE had a violation of CIP-007-3a R3 for failing to assess security patches for applicability within 30 calendar days of availability.

Texas RE determined the duration of the violation to be from the date when URE first failed to address a patch through when URE addressed the outstanding patches.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. These devices were located in a secure room within a secure URE facility that was monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop and implement a biweekly patch remediation process for the devices;

[5] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012968.

2. develop and implement a new security patch management process; also, communicate the process to the relevant team to ensure a common understanding of security patch management as it applies to the servers;
3. evaluate and implement enhancements to the security patch management section of the change management procedure;
4. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of noncompliance and to develop other related improvements;
5. develop and implement a security patch management assessment desktop procedure to facilitate a consistent approach and consistent documentation;
6. develop a cross-functional training program, training materials, and schedule to implement enhanced process and procedure improvements; and
7. establish periodic operational and corporate level controls to ensure security patch management assessment and documentation is conducted and documented in accordance with URE procedures.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-3a R3 (R3.2) (TRE2013012971)

During the Compliance Audit, Texas RE discovered that URE was in violation of CIP-007-3a R3. Specifically, URE installed eight security patches on a server, but it did not complete documentation of the implementation of the patches.

Texas RE determined that URE had a violation of CIP-007-3a R3 for failing to document the implementation of security patches.

Texas RE determined the duration of the violation to be from the date URE installed patches but did not complete documentation of the implementation through when URE documented its implementation of the patches.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although its test plan documentation was deficient, Texas RE determined that URE's servers were shown to have security patches applied. URE testing personnel verified and signed

off on test plan results for cybersecurity controls modification. In addition, URE uses multiple layers of defense, including the use of intrusion prevention systems, firewalls, and network segmentation. URE has strong defenses for external cyber-attacks, and internally there is a substantial effort to reduce risk for internal attacks, viruses, and malware.

To mitigate this violation, URE:[6]

1. documented its implementation of security patches;
2. amended its patch management procedures;
3. reviewed Compliance Audit results and reinforced focus on compliance in the department; and
4. reassigned information technology operational expertise to the relevant team as part of a phased approach to organizational realignment.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R4 (TRE2012010877)

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R4. URE did not have antivirus and malware protection software installed on six devices and three servers. These nine devices are Cyber Assets within the ESP.

Texas RE determined that URE had a violation of CIP-007-1 R4 for failing to have antivirus and malware prevention software installed on nine Cyber Assets within the ESP.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed installing antivirus and malware prevention software on the nine affected devices.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and

[6] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012971.

investigated. In addition, the affected devices were physically located in a secure room within a secure URE facility that was monitored at all times.

To mitigate this violation, URE:[7]

1. installed antivirus and malware prevention software on the affected devices, confirmed the installation of the software on those devices, and confirmed that antivirus and malware prevention software was installed on all other Cyber Assets within URE's ESP;
2. reviewed the antivirus and malware protection procedure and the change management procedure, developed enhancements for those procedures, and developed related desktop procedures;
3. developed and implemented new training for employees responsible for tasks in the new and enhanced procedures;
4. conducted annual NERC compliance training for all employees responsible for implementing and sustaining compliance with Reliability Standards;
5. conducted quarterly CIP awareness sessions to review highlights of industry activity and enhancements in program (ongoing); and
6. implemented a monthly process in which signature update files are validated on all Cyber Assets in the ESPs administered by the relevant team. The process includes a step for a second team member to review and validate the results.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-3a R4 (R4.2) (TRE2013012972)

During the Compliance Audit, Texas RE discovered that URE did not implement its process for updating antivirus signatures for three of its servers. These three servers lost their client relationship with the managing server to receive virus definition updates.

Texas RE determined that URE had a violation of CIP-007-3a R4 for failing to implement its process for the update of antivirus and malware prevention signatures.

[7] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2012010877.

Texas RE determined the duration of the violation to be from the date when the first of the three servers lost its client connection to the antivirus update server through the date when the last of the three servers' client connection was restored and antivirus signatures were updated.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. While these servers were not protected with the latest antivirus and malware prevention signatures during the specified period, URE used multiple layers of defense for compensating measures. URE has strong defenses for external cyber-attacks, and internally there is a substantial effort to reduce risk for internal attacks, viruses, and malware.

To mitigate this violation, URE:[8]

1. updated signatures on the three servers; and
2. updated and implemented its antivirus and malware prevention procedures.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R5 (R5.1, R5.2, R5.3.3) (TRE2013012234)

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R5 in several instances. URE's shared and default account access list did not contain a complete listing of all shared and default accounts and associated access privileges for the Cyber Assets in the ESPs. In addition, URE did not change passwords to all shared and default accounts for the Cyber Assets in the ESPs on an annual basis. This issue affected Cyber Assets administered by a specific URE team.

Texas RE determined that URE had a violation of CIP-007-1 R5 for failing to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE created a comprehensive user access list for shared and default accounts and changed all shared and default account passwords.

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure could have resulted in unauthorized access

[8] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012972.

to URE's Cyber Assets and put URE's system at risk. Inadequate password requirements and failure to ensure password changes could have increased the risk of unauthorized individuals with malicious intent gaining access to URE's Cyber Assets. A complete listing of all shared and default accounts and associated access privileges for the Cyber Assets in the ESPs had never been created. The identified list of default accounts provided as part of the cyber vulnerability assessment was incomplete. The risk was further increased because the list was missing almost half of accounts. The accounts that were identified as missing from the list included default accounts with strong controls and disabled accounts.

However, the risk was mitigated by the following factors. URE limited access to the affected Cyber Assets to a small group of employees and contractors whose access rights were closely monitored by the team's manager. The Cyber Assets themselves were located in protected ESPs behind secure PSPs. Cyber and physical access rights to CCAs in the ESP were being monitored and managed through timely employment status alerts and associated timely access revocation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. create a new, comprehensive user access list for shared and default accounts;
2. change passwords on all Cyber Assets and CCAs with shared/default accounts in the ESPs administered by the relevant team;
3. update its responsibilities matrix procedure to help ensure the requirements of CIP-007 R5 are met;
4. train appropriate personnel on the updated procedure; and
5. implement the updated procedure and post it to the compliance database to facilitate access by appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-2a R9 (TRE2012011180)

URE submitted a Self-Certification stating that it was in violation of CIP-007-2a R9. URE subsequently submitted a more detailed Self-Report stating that it failed to update its change management

procedure within 30 calendar days of a change being completed. Specifically, URE implemented its change management system on one date, but it did not update a section of its procedure until over a year later.

Texas RE determined that URE had a violation of CIP-007-2a R9 for failing to document changes resulting from modifications to systems or controls within 30 calendar days of the change being completed.

Texas RE determined the duration of the violation to be from the date by which URE should have amended its documentation through when URE amended its documentation.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did implement the new system and documented the implementation in its procedure document. However, URE failed to update an additional section of its procedure, the disposal and redeployment section, to reflect the use of the change management system. There were no disposals or redeployments of Cyber Assets administered by the relevant team during the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update its change management procedure to reflect implementation of URE's change management system, post the procedure to its compliance database to facilitate access by appropriate personnel, implement the procedure, and issue an email communication to applicable personnel;
2. conduct training on the revised procedure with all applicable personnel;
3. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of the noncompliance and to develop other related improvements;
4. review the revised procedure and associated training for accuracy and completeness; and
5. establish periodic operational and corporate level controls to ensure documentation updates.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-008-3 R1 (R1.2) (TRE2012011181)

URE submitted a Self-Certification stating that it was in violation of CIP-008-3 R1. URE subsequently submitted a more detailed Self-Report. URE reported that its Cyber Security Incident response plan did not reflect all appropriate personnel updates. Specifically, the text of the plan was not revised to reflect the position changes that were included on URE's list of people to be contacted in the event of an incident (this list was attached to the plan). URE does include a process for updating its plan within 30 calendar days, but URE failed to update contact changes within 30 days according to its process.

Texas RE determined that URE had a violation of CIP-008-3 R1 for failing to reflect personnel updates in its Cyber Security Incident response plan.

Texas RE determined the duration of the violation to be from when the Cyber Security Incident response plan did not reflect all personnel updates through when URE updated the plan to reflect all appropriate personnel updates.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In the event of an incident, the relevant manager would have notified the personnel on the contact list who would have communicated with the appropriate personnel on their respective teams. Additionally, the contact information was correct for most of the people on the incident response team. Lastly, URE did not experience an incident requiring the use of the contacts list during the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update the Cyber Security Incident response plan contact list, post the plan to the compliance database to facilitate access by applicable personnel, implement the plan, and issue an email to appropriate personnel;
2. conduct training on the revised plan with all applicable personnel;
3. update the plan's investigation requirements, post the plan to the compliance database, and issue an email to applicable personnel;
4. conduct training on the revised plan with all applicable personnel;

5. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of noncompliance and develop other related improvements as appropriate; and
6. review the revised plan and associated training to evaluate potential enhancements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Texas RE has assessed a penalty of one hundred and six thousand dollars ($106,000) for the referenced violations. In reaching this determination, Texas RE considered the following factors:

1. Texas RE did not consider URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations which Texas RE considered a mitigating factor;
3. URE self-reported several of the violations;
4. in addition to the mitigating activities described above, URE has undertaken actions beyond those necessary to come into compliance with the Standards. URE continues to implement its self-assessment program, making several enhancements;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations posed a minimal or moderate risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, Texas RE determined that, in this instance, the penalty amount of one hundred and six thousand dollars ($106,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2014 and approved 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 factors considered by Texas RE, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and six thousand dollars ($106,000) 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

REMOVED FROM THIS PUBLIC VERSION

[9] *See* 18 C.F.R. § 39.7(d)(4).

[10] *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).

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 Derrick Davis* Director, Enforcement, Reliability Standards & Registration Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4923 (512) 233-2233 – facsimile derrick.davis@texasre.org	Sonia C. Mendonça* Associate General Counsel and Senior 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* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Rachel Coyne* Enforcement Analyst, Sr. Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4956 (512) 233-2233 – facsimile rachel.coyne@texasre.org

Abby Fellinger* Enforcement Analyst Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4927 (512) 233-2233 – facsimile abby.fellinger@texasre.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.	

Conclusion

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

Respectfully submitted,

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

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior 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