PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 2015

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# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into Settlement Agreements to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreements, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under

[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 (2015). *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.

the terms and conditions of the Settlement Agreements. 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 two Settlement Agreements, one resolving 15 CIP violations and the second resolving 3 TOP-006-2 violations. The details of the findings and basis for the penalty are set forth in the Settlement Agreements and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreements 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 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreements, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013013201	CIP-005-1	R1: R1.5	Medium/ Severe	$150,000
RFC2013013202	CIP-005-1	R2: R2.1, R2.2	Medium/ Severe	
RFC2013013203	CIP-005-1	R3: R3.2	Medium/ Severe	
RFC2013013204	CIP-005-1	R4	Medium/ Severe	
RFC2013013205	CIP-006-1	R1:R1.8	Medium/ Severe	
RFC2013013206	CIP-007-1	R1	Lower/ Severe	
RFC2013013207	CIP-007-1	R2: R2.1, R2.2	Medium/ Severe	
RFC2013013208	CIP-007-1	R3: R3.2	Lower/ Severe	
RFC2013013254	CIP-007-3a	R3	Lower/ Severe	
RFC2013013209	CIP-007-1	R4: R4.1	Medium/ Severe	
RFC2013013210	CIP-007-1	R5: R5.1.2, R5.2	Medium/ Severe	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013013211	CIP-007-1	R6: R6.1, R6.2, R6.4, R6.5	Medium/ Severe	$150,000
RFC2013013212	CIP-007-1	R7	Lower/ Severe	
RFC2013013213	CIP-007-1	R8: R8.1, R8.2, R8.3	Medium/ Severe	
RFC2013013214	CIP-009-1	R5	Lower/ Severe	
RFC2013013251	TOP-006-2	R1	Medium/ Severe	
RFC2013013252	TOP-006-2	R2	High/ Severe	
RFC2013013253	TOP-006-2	R5	Medium/ Severe	

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

Background

ReliabilityFirst conducted a Compliance Audit of URE (Compliance Audit), during which ReliabilityFirst discovered 14 violations of the CIP Reliability Standards. In addition, URE submitted four Self-Reports to ReliabilityFirst stating it was in violation of CIP-007 R3 and TOP-006-2 R1, R2, and R5. ReliabilityFirst and URE negotiated the subject matter of two Settlement Agreements simultaneously, and the penalty associated with the CIP Settlement Agreement includes the assessment of the three TOP-006 violations. NERC staff determined that it was appropriate to process the two separate agreements as a single non-public Notice of Penalty because the facts and circumstances of the three TOP-006-2 violations stemmed directly from the CIP-007 R3 violation.

ReliabilityFirst determined that all of the violations at issue in this Agreement, taken together, except CIP-007-1 R7, posed a serious and substantial risk to reliability. However, ReliabilityFirst determined that it was not necessary to issue a Remedial Action Directive for the violations because URE immediately designed an aggressive, comprehensive Mitigation Plan through which it adopted an entirely new CIP Compliance Program, as described in further detail in the Settlement Agreements.

ReliabilityFirst determined that at the time these violations occurred, URE lacked subject matter experts trained in CIP compliance, and the entity's operating personnel were not required to observe or were not aware of the applicable compliance practices. ReliabilityFirst determined that insufficient management oversight contributed to these issues. ReliabilityFirst determined that if URE had

performed certain key management practices, especially risk management, URE could have reduced the number and severity of its violations.

URE submitted its Mitigation Plan to address the CIP violations to ReliabilityFirst. URE recognized the severity of the risk posed by the subject violations and designed a single, holistic Mitigation Plan that encompassed all of the violations. URE implemented an entirely new CIP Program rather than attempting piecemeal mitigation of the noncompliance. URE has taken certain actions in this Mitigation Plan that address compliance with the multiple violations at once. URE's Mitigation Plan required URE to:

1. verify its Critical Cyber Asset (CCA) inventory by performing a physical walk-down of all Electronic Security Perimeters (ESPs);
2. conduct training for URE staff on revised policies and procedures, including creating and maintaining detailed review and approval schedules for compliance documents;
3. ensure all personnel attend training sessions to discuss the redesigned policies and procedures which apply to their functional areas;
4. reinforce new procedural tasks through task execution; and
5. identify key individuals who will serve as primary points of contact for questions regarding modified policies and procedures.

URE certified that the above Mitigation Plan requirements were completed.

This Full Notice of Penalty will address the portions of the Mitigation Plan that address each of the specific individual violations within the description of each violation below.

CIP-005-1 R1 (RFC2013013201)

During the Compliance Audit, ReliabilityFirst determined that URE failed to provide adequate protection to electronic access control and monitoring (EACM) Cyber Assets engaged in the access control or monitoring of an ESP. Specifically, URE failed to provide the following protective measures of CIP-007: cyber security testing procedures (R1), security patch management (R3), account management (R5.1.2, R5.2.1, R5.2.2, and R5.2.3), EACM disposal or redeployment procedures (R7), and Cyber Vulnerability Assessments (CVAs) (R8.1, R8.2, and R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through the date URE completed its mitigating actions for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the risk was increased because URE had no compensating measures in place and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. document and implement all procedures related to the referenced requirements of cyber security testing procedures (R1), security patch management (R3), account management (R5.1.2, R5.2.1, R5.2.2, and R5.2.3), EACM disposal or redeployment procedures (R7), and CVAs (R8.1, R8.2, and R8.3); and
2. ensure that all EACMS are appropriately included in the scope of these procedures as they are completed in the remaining steps of this Mitigation Plan.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (RFC2013013202)

During the Compliance Audit, ReliabilityFirst determined URE failed to provide adequate evidence of documented organizational processes for control of electronic access at all electronic access points to the ESP. First, URE did not have a documented organizational process for controlling electronic access at all electronic access points to the ESP by enabling only ports and services required for operations and monitoring. Second, URE disallowed inbound traffic through its firewall, but outbound Internet Protocol traffic was set to "permit by default" rather than "deny by default" (R2.1). Third, URE did not enable only ports and services required for operations and for monitoring Cyber Assets within the ESP (R2.2).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through the date URE completed its mitigating actions for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to limit routable communication across the access points to the ESP weakened the defense required for protection of CCAs. URE did not restrict outbound traffic from one of its ESPs, creating the opportunity for a compromised asset to communicate freely with a command and control server or other non-approved device. URE had no compensating measures in place, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. ensure that all ESP access points are configured to deny access by default;

2. document and implement procedures to ensure compliance with CIP-005 R2;
3. clearly document operational necessity for ports and services at ESP access points; and
4. revise access point configuration to limit ports and services to only those required.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R3 (RFC2013013203)

During the Compliance Audit, ReliabilityFirst determined URE failed to have a documented process for monitoring and logging access at access points to the ESP. In addition, URE did not monitor attempts at or actual unauthorized accesses (R3.2) and only monitored failed login attempts.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to monitor and log access to an ESP can result in undetected attacks on the ESP and undetected compromise of assets within the ESP. Failure to alert on unauthorized access attempts may result in an insufficient or untimely response to attacks on the ESP. URE had no compensating measures in place to reduce these risks, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-005 R3;
2. develop and implement a procedure to monitor system events related to cyber security;
3. ensure each ESP access point is configured for security event logging and monitoring;
4. verify that all Cyber Assets within an ESP are adequately monitored for security events, and verify the configuration of automated or manual alerts for systems related to its energy control system (ECS);
5. ensure alerts are generated for unauthorized access attempts and actual unauthorized access; and
6. maintain logs relating to system events for ECS, as well as evidence of the log reviews for ninety calendar days.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (RFC2013013204)

During the Compliance Audit, ReliabilityFirst determined URE failed to include all required elements in its CVAs. URE's annual CVA did not include a review of ports and services (R4.2), discovery of access points to the ESP (R4.3), and a review of controls for default accounts, passwords, and network management community strings (R4.4). In addition, URE did not have a document identifying the CVA process (R4.1) or clear documentation of the results of the CVAs (R4.5).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to perform an adequate CVA kept URE from examining its security practices and identifying necessary improvements. URE had no compensating measures in place, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. implement procedures to ensure compliance with CIP-005 R4;
2. document clearly that an annual CVA has been performed;
3. verify that the annual CVA includes all Cyber Assets within the ESP(s), EACMs, Physical Access Control Systems (PACS) and access points and that only ports and services required for operation are enabled;
4. document clearly a review of controls for default accounts and verify that the annual CVA includes a review of ports and services, discovery of access points to the ESP, and a review of controls for default accounts, passwords, and community strings; and
5. document the results of the CVA and an action plan to address findings.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-1 R1.8 (RFC2013013205)

During the Compliance Audit, ReliabilityFirst determined URE failed to provide adequate protective measures for Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP). URE failed to afford its PACS that authorize and/or log access to the PSPs the following protective measures of CIP-007: cyber security test procedures (R1.3), ports and services processes (R2.1 and

R2.2), security patch management (R3.2), account management (R5.1.2, R5.2.1, and R5.2.3), security status monitoring (R6.1), and CVAs (R8.1, R8.2, and R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the Cyber Assets at issue could be compromised allowing unauthorized access to the CCAs and PSPs. Although the PACS did not reside within the ECS ESP, the PACS did reside within the URE corporate network, which the corporate internal and external intrusion prevention systems protected. The PACS was also behind the corporate firewall, which has a deny-all rule in place as a default. Finally, URE utilized a managed security service provider for the PACS to establish a method of generating and maintaining logs of sufficient detail to create historical audit trails of individual user access activity for a minimum of ninety days.

URE's Mitigation Plan required URE to:

1. document and implement all procedures related to the requirements referenced in CIP-006-3 R2.2; and
2. ensure that all PACS are appropriately included in the scope of these procedures.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (RFC2013013206)

During the Compliance Audit, ReliabilityFirst determined URE failed to create, implement, and maintain cyber security test procedures for all Cyber Assets within the ESP, document that it performs testing that reflects the production environment, and document the test results. URE did not have a clearly defined test procedure for Cyber Assets within the ESP (CIP-007-1 R1.1) and EACM Cyber Assets (CIP-005-1 R1.5). URE did not clearly document that it performed testing in a manner that reflected the production environment (CIP-007-1 R1.2). URE did not document test results for new Cyber Assets and significant changes to existing Cyber Assets within the ESP (CIP-007-1 R1.3), EACM Cyber Assets (CIP-005-1 R1.5), and Cyber Assets that authorize and/or log access to the PSP (CIP-006-3c R2.2).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, inadequate testing of the impact of changes on cyber security controls exposed protected assets to higher risk of compromise. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R1 by creating, implementing, and maintaining adequate test procedures for all Cyber Assets residing within the ESP, EACMs, and PACS;
2. test procedures to ensure testing of security controls required by CIP-005-3 and CIP-007-3; and
3. document that testing performed is representative of the production environment.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R2 (RFC2013013207)

During the Compliance Audit, ReliabilityFirst determined URE failed to establish, document, and implement a process to ensure only those ports and services required for normal and emergency operations are enabled for Cyber Assets within the ESP (CIP-007-1 R2) and Cyber Assets that authorize and/or log access to the PSP (CIP-006-3c R2.2). Accordingly, URE failed to enable only those ports and services required for normal and emergency operations and disable other ports and services.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failing to keep the number of listening ports and active services at a minimum exposed URE's Cyber Assets to a greater risk of compromise. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R2;
2. document clearly that only ports and services required for normal and emergency operations are enabled for all Cyber Assets within the ESP; and
3. document clearly that ports and services not required for operations or monitoring are disabled prior to production use.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-3 R3 (RFC2013013208)

During the Compliance Audit, ReliabilityFirst determined URE failed to implement a patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for Cyber Assets within the ESP. URE also failed to provide sufficient evidence of the implementation of security patches for Cyber Assets within the ESP, EACM devices, and PACS devices. URE did not monitor certain sources of software patches for Cyber Assets within the ESP, EACM devices, and PACS devices.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to implement properly a security patch management system made URE vulnerable to infiltration from outside entities. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. document clearly the assessment of all security patches for all applicable assets and for all applicable patch sources as required; and
2. schedule security patches for installation in accordance with URE policy.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R4 (RFC2013013209)

During the Compliance Audit, ReliabilityFirst determined URE failed to use antivirus software or malicious software prevention tools on all Cyber Assets within the ESP. In addition, URE failed to document and implement antivirus and malware prevention tools and failed to document and implement compensating measures used to mitigate risk exposure in cases where it did not install antivirus software and malware prevention tools.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the failure left the organization vulnerable to viruses and malware. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R4;
2. document clearly that antivirus software and malicious software prevention tools are used on all Cyber Assets within the ESP; and
3. develop and implement compensating and mitigation measures for those Cyber Assets that are not capable of running antivirus or malware prevention tools.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R5 (RFC2013013210)

During the Compliance Audit, ReliabilityFirst determined URE failed to 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. ReliabilityFirst identified four instances of noncompliance. First, URE provided evidence that it was logging security events, but URE failed to create historical audit trails of individual account access activity (R5.1.2). Second, for Cyber Assets within the ESP, EACM devices, and PACS devices, URE failed to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges (R5.2). Third, for Cyber Assets within the ESP and EACM devices, URE failed to identify individuals or roles with access to shared accounts (R5.2.3). Finally, for Cyber Assets within the ESP and EACM devices, URE failed to establish an audit trail of shared account use or steps for securing the account in the event of personnel changes (R5.2.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE's failures increased the likelihood for unauthorized system access and decreased the likelihood that URE would detect an unauthorized system access. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R5;
2. document clearly historical audit trails for individual user account access activity for Cyber Assets, EACMs, and PACs;
3. develop and implement a policy that minimizes and manages the scope and acceptable use of administrative, shared, and other generic account privileges; and
4. document clearly audit trails of account use and the procedural steps to secure the accounts in the event of personnel changes.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R6 (RFC2013013211)

During the Compliance Audit, ReliabilityFirst determined URE failed to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor cyber security-related system events for approximately four years. In addition, URE failed to ensure that all Cyber Assets within an ESP were monitoring for security events (R6.1) and failed to configure monitoring systems to issue automated or manual alerts for ECS (R6.2). Furthermore, URE failed to demonstrate that it retained logs for 90 calendar days (R6.4) and failed to provide evidence of the review of logs related to system events for ECS (R6.5).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE's failure to monitor cyber security-related system events decreased the likelihood that URE would detect a potential compromise on the system. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R6;
2. develop and implement a procedure to monitor system events related to cyber security;
3. ensure that each ESP access point is configured for security event logging and monitoring;
4. verify that all Cyber Assets within an ESP are adequately monitored for security events;

5. verify the configuration of automated or manual alerts for ECS;
6. ensure alerts are generated for unauthorized access attempts and actual unauthorized access; and
7. maintain logs relating to system events for ECS, as well as evidence of the log reviews, for 90 calendar days.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R7 (RFC2013013212)

During the Compliance Audit, ReliabilityFirst determined URE failed to establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP. URE provided a policy, which stated URE has established formal methods, policies, and procedures for disposal of Cyber Assets within the ESP. However, the policy did not provide such methods, policies, and procedures.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Despite not having formal documentation in place, URE was disposing of and redeploying Cyber Assets within the ESP according to the Standard. URE kept assets removed from service in a physically secure environment. While URE did not maintain an inventory list, there was restricted access to the area where the equipment was being stored, and URE developed an inventory list prior to sending any items for destruction.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R7; and
2. develop and implement formal disposal or redeployment processes and procedures for Cyber Assets within the ESP.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R8 (RFC2013013213)

During the Compliance Audit, ReliabilityFirst determined URE failed to document its CVA process for one year (R8.1), conduct a review to verify that only ports and services required for operation are enabled (R8.2), and conduct a review of controls for default accounts (R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE did not have sufficient awareness of the vulnerabilities of its ESP access points or Cyber Assets within the ESP, and therefore was more vulnerable to attack. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-005 R4 and CIP-007 R8;
2. document clearly that an annual CVA has been performed;
3. verify that the annual CVA includes all Cyber Assets within the ESP(s), EACMs, PACs and access points and that only ports and services required for operation are enabled;
4. document clearly a review of controls for default accounts and verify that the annual CVA includes a review of ports and services, discovery of access points to the ESP, and a review of controls for default accounts, passwords, and community strings; and
5. document the results of the CVA and draft an action plan to address findings.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R5 (RFC2013013214)

During the Compliance Audit, ReliabilityFirst determined URE failed to demonstrate it annually tested the backup media containing information essential for the recovery of CCAs. For its ECS operations area, URE had a procedure to perform information backups on various types of CCAs, but URE failed to demonstrate it annually tested its backup media that contains information essential for the recovery of CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, while URE had information essential to the recovery of CCAs on backup media, URE did not test the backup media annually and had no assurance that it could use this backup media to recover CCAs if necessary. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-009 R5; and
2. conduct and clearly document an annual test of backup media that contains information essential for the recovery of CCAs.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-3a R3 (RFC2013013254), TOP-006-2 R1 (RFC2013013251), R2 (RFC2013013252), and R5 (RFC2013013253)

URE submitted four Self-Reports to ReliabilityFirst stating it had violations of CIP-007-3a R3 and TOP-006-2 R1, R2, and R5. A URE transmission operations control center (TOCC) experienced an ECS failure lasting approximately 91 minutes during which the TOCC lost monitoring and control capabilities. The root cause of this particular service interruption was that URE had not assessed an upgrade released at the time of the ECS outage. Following the ECS outage and the Compliance Audit, URE discovered that it evaluates antivirus software patches, but does not track, evaluate, test, and install all software patches (R3). In addition, URE did not satisfactorily identify and describe compensating measures applied to mitigate risk exposure when it fails to install a security patch.

URE violated TOP-006-2 R1 by failing to monitor the status of all transmission resources available for use and failed to inform the Reliability Coordinator of all available transmission resources. URE violated TOP-006-2 R2 by failing to monitor applicable transmission line status, real and reactive power flows, voltage, and status of rotating and static reactive resources. URE violated TOP-006-2 R5 by not using monitoring equipment to communicate to operating personnel any important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.

ReliabilityFirst determined the duration of the CIP-007-3a R3 violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined the duration of the three TOP-006 violations to be 91 minutes on the day of the incident, when it lost the ability to monitor due to the ECS failure.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the inadequately tested patch caused a service interruption for approximately 91 minutes. There was no real-time, accurate data for URE to transmit due to the ECS issues. URE lost BPS visibility and monitoring for approximately 91 minutes.

Throughout the event, URE maintained communication with its Reliability Coordinator, neighboring Transmission Operators, and all URE generating plants to ensure monitoring of the system. The interconnecting Transmission Operators monitored the URE system during the event. URE followed its emergency operating plans for loss of control center functionality to assess and respond to the event.

URE mitigated the CIP-007 R3 violation through the holistic CIP Mitigation Plan with the same actions as listed above in the CIP-007 R3 (RFC2013013208) description.

URE's Mitigation Plan to address the TOP violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. develop a plan to assess and improve the backup control center functionality, including developing a plan to connect remaining non-critical Remote Terminal Units to the backup ECS and install backup communications system hardware, including fiber optic cables;
2. include in the plan automating steps to transfer communications to backup control centers;
3. enhance synchrophasor usage, including adding phasor data collector server hardware at the backup control center, fully replicating synchrophasor functionality at the backup control center, and creating user screens and views to enhance situational awareness;
4. add redundant synchrophasor monitoring replicating the primary control center, which when acting together with automating communications to the backup control center, will reduce time delays to disable the primary system and activate the backup system as well as increase operators' situational awareness;
5. provide training to its TOCC operators relating to synchrophasors; and
6. review and improve operations technology on-call and operator procedures, enhance the ECS dashboard, and train operations technology support and TOCC operators on revised procedures and the ECS dashboard.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreements, ReliabilityFirst has assessed a penalty of one hundred fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered 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 ReliabilityFirst considered a mitigating factor;
3. URE self-reported the violations of CIP-007-3a R3 and TOP-006-2 R1, R2, and R5;
4. 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. ReliabilityFirst determined that the violations, considered together (with the exception of CIP-007-1 R7), posed a serious and substantial risk to the reliability of the BPS and indicated a systematic performance failure by URE;
7. URE committed to a comprehensive Mitigation Plan with an aggressive completion schedule. URE also agreed to complete significant above-and-beyond action items to establish a culture of compliance and high level of reliability protection consistent with good utility practices;
8. since URE's Compliance Audit, URE has made significant improvements to its CIP compliance program. To confirm that URE's new CIP Compliance Program is performing as designed, ReliabilityFirst and URE have also agreed that ReliabilityFirst will conduct a Spot Check of URE;
9. URE volunteered to have ReliabilityFirst conduct an on-site appraisal for the management practices associated with risk management, external interdependencies, asset and configuration management, information management, implementation, integration, validation, and verification. ReliabilityFirst will evaluate and measure URE's implementation of management controls, processes, worker knowledge and skills, and technology relating to these management practices. In the event ReliabilityFirst identifies areas of improvement during the appraisal, URE will develop action plans and provide ReliabilityFirst with quarterly updates regarding the progress of these plans; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred fifty thousand dollars ($150,000) 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[4]

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,[5] the NERC BOTCC reviewed the Settlement Agreements and supporting documentation on April 13, 2015 and approved the Settlement Agreements. In approving the Settlement Agreements, 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 also considered the factors considered by ReliabilityFirst as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreements and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) 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

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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 Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Deputy General Counsel, Vice President of Compliance and 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 Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org

Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org Kristen Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0669 (216) 503-9207 facsimile kristen.senk@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.	

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
Deputy General Counsel, Vice President of
Compliance and 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
ReliabilityFirst Corporation