PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

September 28, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 2042

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP12-_-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 Florida Reliability Coordinating Council, Inc. (FRCC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from FRCC's determination and findings of the violations[3] of CIP-004-1 R4, CIP-007-1 R1, CIP-006-2 R5, CIP-007-1 R3, CIP-005-1 R2.2, CIP-007-1 R2, CIP-007-1 R8, CIP-005-1 R4.5, CIP-006-1 R6, CIP-007-1 R3, CIP-007-1 R5, and CIP-007-1 R6. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred and fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers FRCC200900304, FRCC201000312, FRCC201000377, FRCC201000378, FRCC201100420, FRCC201100421, FRCC2011007241,

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

2 See 18 C.F.R § 39.7(c)(2).

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

FRCC2011007252, FRCC2011007256, FRCC2011007257, FRCC2011007259, and FRCC2011007260 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on July 31, 2012, by and between FRCC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Florida Reliability Coordinating Council, Inc.	Unidentified Registered Entity	NOC-1552	FRCC200900304	CIP-004-1	R4	Lower[4]	$150,000
			FRCC201000312	CIP-007-1	R1	Medium[5]	
			FRCC201000377	CIP-006-2	R5	Medium[6]	

[4] CIP-004-1 R4 and R4.1 each have a Lower Violation Risk Factor (VRF); R4.2 has a Medium VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

[5] CIP -007-1 R1 has a Medium VRF and CIP-007-1 R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-007-1 R1.1 was in effect from July 1, 2008 until January 27, 2009 when the Medium VRF became effective.

[6] CIP-006-1 R5 has a Lower VRF and CIP-006-2 R5 has a Medium VRF. CIP-006-1 VRFs were in effect from June 18, 2007 through March 31, 2010 and CIP-006-2 VRFs were in effect from April 1, 2010 through September 30, 2010.

			FRCC201000378	CIP-007-1	R3	Lower	
			FRCC201100420	CIP-005-1	R2.2	Medium[7]	
			FRCC201100421	CIP-007-1	R2	Medium[8]	
			FRCC2011007241	CIP-007-1	R8	Medium[9]	
			FRCC2011007252	CIP-005-1	R4.5	Medium[10]	
			FRCC2011007256	CIP-006-1	R6	Medium[11]	
			FRCC2011007257	CIP-007-1	R3	Lower	

[7] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a Medium VRF; R2.5 and its sub-requirements and R2.6 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-005-1 R2 and R2.4 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRFs for CIP-005-1 R2 and R2.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

[8] When NERC filed VRFs it originally assigned CIP-007-1 R2 and R2.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R2 and R2.3 were in effect from July 1, 2008 until February 2, 2009, when the Medium VRFs became effective.

[9] CIP-007-1 R8 and R8.1 each have a Lower VRF; R8.2, 8.3 and 8.4 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-007-1 R8.2, 8.3 and 8.4 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRFs for CIP-007-1 R8.2, 8.3 and 8.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

[10] CIP-005-1 R4, R4.2, R4.3, R4.4 and R4.4 each have a Medium VRF; R4.1 has a Lower VRF. When NERC filed VRFs it originally assigned CIP-005-1 R4, R4.2, R4.3, R4.4 and R4.4 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRFs for CIP-005-1 R4, R4.2, R4.3, R4.4 and R4.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

[11] CIP-006-1 R6 and R6.1 each have a Medium VRF; R6.2 and R6.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-006-1 R6.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 6.1 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective.

			FRCC2011007259	CIP-007-1	R5	Medium[12]	
			FRCC2011007260	CIP-007-1	R6	Medium[13]	

FRCC200900304 (CIP-004-1 R4)

The purpose statement of Reliability Standard CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of Standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity[14] shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change

[12] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF. When NERC originally filed VRFs it originally assigned CIP-005-1 R5.1 and R5.3.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on August 20, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-005-1 R5.1 and R5.3.3 were in effect from June 18, 2007 until August 20, 2009, when the Medium VRFs became effective.

[13] When NERC filed VRFs it originally assigned CIP-007-1 R6.1, R6.2 and R6.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R6.1, R6.2 and R6.3 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective. CIP-007-1 R6, R6.4 and R6.5 each have a Lower VRF; R6.1, R6.2 and R6.3each have a Medium VRF.

[14] Within the text of Standard CIP-004, CIP-005, CIP-006 and CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
>
> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 Hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL).

As part of its continuing improvement process to ensure compliance with the applicable CIP Standards, URE found a possible noncompliance with this Standard by comparing the list of personnel who were authorized for such access and the list of personnel who were actually granted such access. In advance of a Spot Check, URE self-reported that after conducting an internal review of its compliance with CIP-004, URE found that 33 individuals who did not have authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) were included on the list of authorized personnel with access to these CCAs, in violation of CIP-004-1 R4. FRCC determined that the 33 individuals represented greater than 10% but less than 15% of URE's personnel with access to the CCAs.

URE has stated that this violation was a result of improper control of access provisioning. URE's review also concluded that its physical access controls were ineffective to meet the CIP-004-1 R4 requirements and a separate physical access control system was required to address compliance with this Standard.

FRCC determined that URE had a violation of CIP-004-1 R4 because URE did not maintain a list of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs, and because URE's physical access controls were ineffective to meet the requirements of this Standard.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, FRCC

determined that lack of accurate listing of authorized personnel could have resulted in compromise of the security of the Electronic Security Perimeters (ESPs) and the Physical Security Perimeters (PSPs). The risk to the BPS was mitigated because URE maintained strong electronic authentication controls and promptly revoked any access upon discovery. Further, the risk was mitigated by the fact that 51.5 % of the individuals at issue did not access the PSPs during the violation timeframe; 76.5% of the individuals had completed the personnel risk assessment (PRA) and the required training and 75% of the remaining individuals had completed the required training but not the PRA. The remaining 48.5% of the individuals were granted access prior to the compliance date and were trusted based on the individual roles and responsibilities they had. These violations resulted from grandfathering of access privileges for the personnel at issue, and all of the individuals had access to the PSPs prior to the compliance date.

FRCC201000312 (CIP-007-1 R1)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

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

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

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

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

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL

During a Compliance Spot, FRCC discovered that URE failed to demonstrate that testing procedures ensured that significant changes to URE's existing Cyber Assets (CAs) within the ESP did not adversely affect existing cyber security controls, in violation of CIP-007-1 R1. URE conducted test procedures for operational sufficiency but failed to conduct tests and document results for cybersecurity tests as required by CIP-007-1 R1. FRCC's Spot Check team reviewed 94.4% of the tests and determined that all 94% of the tests failed to include required elements of testing necessary to counter adverse impact to the existing security controls, such as access control verification, file integrity check, ports and services, review for system security audit function.

FRCC determined that URE had a violation of CIP-007-1 R1 because URE failed to ensure that significant changes to URE's existing CAs within the ESP did not adversely affect existing cybersecurity controls.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that all changes to the existing CAs lacked testing of cybersecurity controls, which could potentially result in gaps in URE's secured environment. The risk to the BPS was mitigated by the fact that all changes to the existing CAs were application and patch upgrades provided and recommended by trusted vendors and included installation directions that specified the configuration approved by the SCADA vendor.

FRCC201000377 (CIP-006-2 R5)

The purpose statement of Reliability Standard CIP-006-2 provides: "Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-006-2 R5 provides:

> R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:
>
> - Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
>
> - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

CIP-006-2 R5 has a "Medium" VRF and a "Severe" VSL.

As part of its continuing improvement process, URE executed a routine evidence review to confirm compliance with the requirements of the NERC CIP Standards. As a result of its review, URE self-reported that it failed to implement controls to ensure that all unauthorized access attempts were reviewed immediately and handled in accordance with the procedures specified in CIP-008-2, as required by CIP-006-2 R5.

Specifically, URE implemented a new physical access control system but did not configure the new system, so that logs are reviewed and/or timely notifications are sent to those responsible for responding to physical security events. URE reported that although its system was logging the appropriate security events, the physical security department did not have the system configured to monitor the logs and send notifications to the individuals responsible for responding to physical security incidents.

The review also determined that the noncompliance existed since the date URE first violated this Standard.

The review determined that the necessary procedures and documentation required by this Standard were both established and disseminated to the appropriate Subject Matter Experts (SMEs) within URE. The investigation also revealed that the cause of the violation was that URE lacked sufficient internal management control to monitor and verify the performance of the SMEs as it relates to compliance with this Standard.

FRCC determined that URE had a violation of CIP-006-2 R5 because URE did not document and implement the technical and procedural controls to ensure that all unauthorized access attempts are reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2.

FRCC determined the duration of the violation to be from the date URE first violated this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined URE's controls were not sufficient to limit potential unauthorized access because prompt alerting and alert response were not implemented. The risk to the BPS was mitigated by the fact that all but one of the PSPs were within the URE compounds for which access was controlled. All front gates to the compounds had badge access, and visitor access was controlled by a guard at the reception, and all visitors were escorted at all times. Further, URE did not discover any attempts for unauthorized access during the pendency of the violation.

FRCC201000378 CIP-007-1 R3.1[15]

CIP-007-1 R3 provides in pertinent part:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking,

[15] FRCC determined that violation FRCC2011007257 is a repeat violation of FRCC201000378. URE self-reported FRCC201000378. Later, during a Spot Check, FRCC discovered that patching was not considered for many applications, in violation of CIP-007-1 R3.

evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

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

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE self-reported that it did not perform or document the assessment of available security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades, as required by CIP-007-1 R3.1. FRCC assessed and determined a total of 89.3% of the patches were not reviewed for applicability within the required period of 30 days, in violation of this Standard.

FRCC determined that URE had a violation of CIP-007-1 R3.1 because URE failed to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades.

FRCC determined the duration of the violation to be from when URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to document the assessment of security patches and security upgrades for applicability exposed the CAs within its ESP to potential cyber vulnerability. The risk to the BPS was mitigated by the fact that all 89.3% of the changes were for Microsoft monthly patch upgrades and other application updates from trusted vendors. While the URE did not assess the patches for applicability, all the patches were required and recommended by the vendor.

FRCC201100420 (CIP-005-1 R2.2)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R2.2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ****
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

CIP-005-1 R2.2 has a "Medium" VRF and a "Severe" VSL.

As part of its continuing improvement process, URE executed a routine evidence review to confirm compliance with the requirements of the NERC CIP Standards. The review determined that the necessary assessment procedures and documentation required by CIP-005 R2 were both established and disseminated to the appropriate SMEs within URE. The investigation also revealed that the cause of the violation was that URE lacked sufficient internal management control to monitor and verify the performance of the SMEs as it relates to this Standard.

URE self-certified that it failed to implement the organizational processes and technical and procedural mechanisms for control of electronic access at all of its electronic access points to its ESP. Specifically, URE could not demonstrate that at all ESP access points, only ports required for operations and monitoring of CAs within the ESP were enabled, as required by this Standard.

URE reported that although it had strong firewall rule sets in place at the access points that strictly limit the applications, ports, and services allowed to traverse the ESP, there was insufficient evidence and documentation to prove that only the required ports and services have been enabled.

FRCC determined that URE had a violation of CIP-005-1 R2.2 because URE failed to enable only ports and services required for operations and for monitoring CAs within the ESPs.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, this violation could potentially lead to intruders exploiting open ports and services for malicious purposes even when only trusted systems were allowed in the ESP. The risk to the BPS was mitigated by the fact that the electronic access points were configured to deny access by default and explicit permissions were specified. Further, URE had strong firewall rule sets at the electronic access points.

FRCC201100421 (CIP-007-1 R2)

CIP-007-1 R2 provides in pertinent part:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE self-certified that it failed to document and establish a process to ensure that only those ports and services required for normal and emergency operations were enabled, as required by CIP-007-1 R2. URE also failed to ensure that only those ports and services required for normal and emergency operations were enabled, as required by CIP-007-1 R2.1.

FRCC determined that URE had a violation of CIP-007-1 R2 because it failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. URE also failed to enable only those ports and services required for normal and emergency operations, as required by CIP-007-1 R2.1.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, this violation could potentially lead to intruders exploiting open ports and services for malicious purpose even when only trusted systems were allowed in the ESP. The risk to the BPS was mitigated by the fact that the CAs at issue were configured as per vendor specifications and to deny access by default, and explicit permissions to the access points were specified.

FRCC2011007241 (CIP-007-1 R8)

CIP-007-1 R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R8.1. A document identifying the vulnerability assessment process;
> >
> > R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
> >
> > R8.3. A review of controls for default accounts; and,
> >
> > R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-1 R8 has a "Medium" VRF and a "Severe" VSL.

URE self-certified that it failed to demonstrate that its annual Cyber Vulnerability Assessment (CVA) conducted for two years included a review to verify that only ports and services required for operation of the CAs within the ESP were enabled, as required by CIP-007-1 R8.2. URE's CVA also failed to include a review of controls for default accounts for all CAs, as required by CIP-007-1 R8.3. Further, URE's CVA did not include evidence of documenting an action plan that included the execution status for all the identified vulnerabilities, as required by CIP-007-1 R8.4.

FRCC determined that URE had a violation of CIP-007-1 R8 because URE's CVA of all CAs within the ESP did not include the minimum requirements for a vulnerability assessment listed in CIP-007-1 R8.2, R8.3 and R8.4.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that a delay in remediation of vulnerabilities for outside trusted systems could potentially be exploited and lead to risks to the ESP. The risk to the BPS was mitigated by the fact that the access points had additional protective measures, limiting the risk of exploitation of ports and services. URE's protective measures included effective deny by default access. Also, all remote access was very limited and secured. All ports and services implemented at the access points were limited to ports that are required for operation. URE also had no default passwords for the CAs in the ESP, which decreased the risk to the BPS. Further, most of the vulnerabilities identified in the CVA were for systems outside the ESP and the vulnerabilities within the ESP were all corrected.

FRCC2011007252 (CIP-005-1, R4.5)

CIP-005-1 R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ****
>
> > R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-1 R4.5 has a "Medium" VRF and a "Severe" VSL.

During a Compliance Spot Check, FRCC discovered that URE failed to demonstrate that it created action plans to remediate or mitigate vulnerabilities identified during two of its CVAs, as required by CIP-005-1 R4.5.

FRCC determined that URE had a violation of CIP-005-1 R4.5 because URE's CVAs at issue did not include an action plan to remediate or mitigate vulnerabilities identified in the CVA.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that a delay in remediation of vulnerabilities for outside trusted systems could potentially be exploited and lead to risks to the ESP. The risk to the BPS was mitigated by the fact that 72.7% of the vulnerabilities identified in the CVA were for systems outside the ESP, and 27.3% of the vulnerabilities were for systems inside the ESP. Further, FRCC determined that none of the vulnerabilities were externally exploitable or could compromise immediate system integrity.

FRCC2011007256 (CIP-006-1 R6)

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

CIP-006-1 R6 provides:

> R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:
>
> > R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
> >
> > R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.
> >
> > R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

CIP-006-1 R6 has a "Medium" VRF and a "Severe" VSL.

During a Compliance Spot Check, FRCC discovered that URE failed to document and implement a maintenance and testing program which ensured that all physical security systems under CIP-006-1 R2, R3, and R4 function properly, as required by CIP-006 R6.[16]

FRCC determined that URE had a violation of CIP-006-1 R6 because it failed to implement the maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that lack of documented maintenance and testing program could result in weak implementation and a potential failure of the physical security controls. The risk to the BPS was mitigated by the fact that URE's vendors provided prompt fixing and testing of all defective systems upon notification. Further, all systems were tested at the time of implementation but the entity failed to maintain documented records of all the testing and maintenance performed during initial implementation.

FRCC2011007257 (CIP-007-1 R3)[17]

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

During a Compliance Spot Check, FRCC discovered that URE failed to document and establish security patch management tracking requirements for multiple applications in use within the ESP. Evidence submitted to FRCC was insufficient to demonstrate that URE was tracking all security patches and performing the assessment for applicability within thirty days from the date of availability. Further, many of the patches were not installed because URE was still in the process of mitigating its lack of adequate testing procedures for many of its CAs, which was self-reported by URE.[18]

[16] The CIP-006 R6 violation spans multiple versions of the Standard, for convenience the Standard will be referred to as CIP-006-1 throughout this document.
[17] The language of this Standard is provided above for violation FRCC201000378.
[18] URE self-reported violation FRCC201000378, which involves the same Standard. FRCC discovered FRCC2011007257 during a Spot Check.

FRCC determined that URE had a violation of CIP-007-1 R3 because it failed to establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all CAs within the ESP.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that because URE did not effectively track and implement controls for security patches and updates for third party systems, URE caused limited exposure of the systems. Most the applications that were not patched were configured to communicate internally only, and therefore limited external exposure of the systems. The risk to the BPS was also mitigated by the fact that a patching program was effectively implemented for all critical applications such as URE's Energy Management System (EMS), Microsoft MS operating systems, and Linux.

FRCC2011007259 (CIP-007-1 R5)

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
>
> ***
>
> R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
>
> ***

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

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

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

***

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

***

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

CIP-007-1 R5 has a "Medium" VRF and a "Severe" VSL.

During a Compliance Spot Check, FRCC discovered that URE failed to review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 R5 and Standard CIP-004-3 R4, as required by CIP-007-1 R5.1.3. URE also failed to document and implement a policy to require change of passwords for default accounts that must remain enabled and cannot be disabled or renamed. Further, URE failed to demonstrate that all default accounts were documented and either disabled or renamed, and where disabling or renaming of accounts was not possible, that passwords had been changed appropriately, as required by CIP-007-1 R5.2.1. URE also failed to identify all individuals with access to its shared accounts, as required by CIP-007-1 R5.2.2.

Further, URE failed to demonstrate that all CAs within the ESP with Microsoft operating systems comply and enforce the password complexity required by CIP-007 R5.3.2. URE did not submit any Technical Feasibility Exception (TFE) requests as per CIP-007 R5.3 for these CAs, nor document mitigating measures to provide comparable security, which is required in the event an entity cannot demonstrate strict compliance with R5.3.2.

FRCC determined that URE had a violation of CIP-007-1 R5 because it failed to: (i) review, at least annually, user accounts to verify access privileges as per R5.1.3; (ii) failed to implement a policy as per R5.2 and to include the requirements of R5.2.1 into its policy; (iii) failed to identify all individuals with access to its shared accounts as per R5.2.2; and (iv) failed to ensure that all CAs within the ESP comply with and enforce the password complexity required by CIP-007 R5.3.2.

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, lack of documentation of shared and administrative account assignments could result in misappropriation of privileges and unauthorized access to the ESP Cyber Assets. The risk to the BPS was mitigated by the fact that all accounts and shared passwords were secured using best industry practices. Further, in cases of termination and transfers of personnel, user access was terminated from the active directory, thus denying any mode of access to the network, and passwords were changed to further limit the risk.

FRCC2011007260 (CIP-007-1 R6)

CIP-007-1 R6 provides in pertinent part:

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

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

CIP-007-1 R6 has a "Medium" VRF and a "Severe" VSL.

During a Compliance Spot Check, FRCC discovered that URE failed to ensure that all of its CAs within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, as required by CIP-007-1 R6. URE failed to implement security monitoring controls that issue automated or manual alerts for detected cybersecurity incidents, as required by CIP-007-1 R6.2. Further, URE failed to provide evidence to demonstrate that for all CAs, it maintained logs of system events related to cyber security to support incident response, as required in Standard CIP-008-3, and in violation of CIP-007-1 R6.3. Finally, URE failed to review the logs of system events related to cyber security and failed to maintain records documenting review of these logs, as required by CIP-007-1 R6.5.

FRCC determined that URE had a violation of CIP-007-1 R6 because it failed to: (i) implement automated tools or organizational process controls to monitor system events; (ii) failed to implement security monitoring controls that issue automated or manual alerts, per R6.2; (iii) failed to show that it maintained logs of system events related to cyber security, per R6.3; and (iv) failed to review the logs of system events related to cybersecurity to maintain records documenting the review, per R6.5

FRCC determined the duration of the violation to be from the date URE was required to comply with this Standard, through when URE completed its Mitigation Plan.

FRCC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the BPS. Specifically, FRCC determined that because the monitoring and alerting for cyber security incidents was not effective for all CAs, an unauthorized person could have had opportunity to access the system. The risk to the BPS was mitigated by the fact that all ESPs were well monitored and logs were maintained, even though they were not reviewed. URE maintained a security event monitoring system for all access points and completed informational level logging records. Further, ESPs were protected and intrusion detection was effective for the ESPs.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, FRCC has assessed a penalty of one hundred fifty thousand dollars ($150,000.00) for the referenced violations. In reaching this determination, FRCC considered the following factors:

1. FRCC applied self-reporting credit for three of the violations included in this Full Notice of Penalty;[19]
2. URE's violation history;
3. FRCC determined that the violation of CIP-007-1 R3 (FRCC2011007257), included in this Full NOP, is a repeat violation of FRCC201000378, which involves the same Standard, and is also included in this Full NOP;
4. URE cooperated during the enforcement process;
5. There was no indication or evidence that URE attempted to conceal the violations;
6. FRCC reviewed URE ICP and based on the responses and documents submitted by URE, it was considered as a neutral factor;
7. FRCC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. FRCC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, FRCC determined that, in this instance, the penalty amount of one hundred fifty thousand dollars ($150,000.00) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[20]

FRCC200900304 (CIP-004-1 R4)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to FRCC on January 6, 2010. The Mitigation Plan was accepted by FRCC on January 8, 2010 and approved by NERC on July 28, 2010. The Mitigation Plan for this violation is designated as MIT-08-2251 and was submitted as non-public information to FERC on July 28, 2010 in accordance with FERC orders.

[19] The violations are as follows: FRCC200900304 (CIP-004-1 R4); FRCC201000377 (CIP-006-2 R5); and FRCC201000378 (CIP-007-1 R3).
[20] See 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. Perform detailed analysis of URE's authorization list and compare it against the physical security database;
2. Perform immediate remediation steps. URE's compliance office reconciled the list of authorized personnel who have access with the physical security database, which logs access that was actually granted. URE also revoked access for all unauthorized individuals;
3. Perform evidence verification for its physical security. URE committed to design and implement a standalone physical security system that is strictly dedicated to the physical access controls related to CIP compliance. The new system reduces the possibility of human error by close to 95%;
4. Analysis of electronic access controls. URE performed analysis of the electronic security controls in addition to the analysis of its physical security controls, and completed an EMS network enhancement project to ensure compliance with CIP Version 2 Standards;
5. Implement an access control program. The program defines the roles and responsibilities of the individuals involved in authorizing, changing and revoking access to the physical security perimeters. It also includes a list of the steps necessary to perform these functions;
6. Evaluate the access control program. URE's compliance committed to evaluate and monitor the performance of the program through a bi-weekly review and comparison of the physical security database against the list of authorized individuals; and
7. Implement the access control program. URE implemented automated reporting capabilities function to its system in order to easily audit and compare the list of individuals with authorized access against the individuals who were actually granted access.

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

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

FRCC201000312 (CIP-007-1 R1)
URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to FRCC on June 24, 2010. The Mitigation Plan was accepted by FRCC on July 19, 2010 and approved by NERC on July 28, 2010. The Mitigation Plan for this violation is designated as MIT-08-2478 and was submitted as non-public information to FERC on July 28, 2010 in accordance with FERC orders. URE submitted multiple extension requests for the Mitigation Plan.

URE's Mitigation Plan required URE to:

1. Document test procedures;
2. Update test procedure control program document;
3. Identify testing configuration environment; and
4. Run security tests and document results.

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

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

FRCC201000377 (CIP-006-2 R5)
URE's Mitigation Plan to address its violation of CIP-006-2 R5 was submitted to FRCC on September 7, 2010. The Mitigation Plan was accepted by FRCC on January 12, 2011 and approved by NERC on January 31, 2011. The Mitigation Plan for this violation is designated as MIT-10-3253 and was submitted as non-public information to FERC on February 3, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement immediate remediation:
    a. Implement temporary measures for monitoring and alerting. URE's security system was configured to email all system generated alarms to the transmission operator's email account, which is manned and monitored 24 hours a day, 7 days a week. Later, the plan was enhanced, so that the system emails the alarms directly to security center, which is also manned and monitored at all times; and

b. Implemented additional procedures related to badge alarms, forced door alarms and door held open alarms.

2. Conduct a three-month monitoring plan:
   a. Perform root cause analysis;
   b. Perform analysis of system alarms;
   c. Perform research to establish ability of the security center to perform monitoring;
   d. Develop evidence reporting methodology;
   e. Develop process flow for monitoring and alerting; and
   f. Enhance security patch management program.

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

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

FRCC201000378 (CIP-007-1 R3)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to FRCC on August 17, 2010. The Mitigation Plan was accepted by FRCC on January 1, 2011 and approved by NERC on January 31, 2011. The Mitigation Plan for this violation is designated as MIT-09-3254[21] and was submitted as non-public information to FERC on February 3, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Perform immediate remediation steps. URE assessed the patches that were released and were not installed;
2. Implement a six-month monitoring plan. URE developed a program for addressing the manner in which the assessment of patches and upgrades to CCAs are conducted. The following actions were taken in connection to this program:
   a. Restructured the EMS staff structure to report to a different business unit with more available management resources to oversee the staff's day-to-day activities;

[21] According to the Mitigation Plan, this violation and the mitigating activities associated with it are closely related to the repeat CIP-007 R3 violation included in this Full NOP.

b. Performed root cause analysis and determined that the necessary assessment procedures and documentation required by this Standard were both established and disseminated to the appropriate staff;

c. Improved existing methodology for notifications. Specific individuals are assigned the responsibility of receiving automated notifications of security patch releases and for regularly checking vendor web sites for updates when an automated means is not available;

d. Improved existing methodology for program execution. URE performed enhancements to existing methods to track patch and update assessments. This was accomplished by using spreadsheets, forms, and procedures to track each patch or update released by each system vendor. This documentation included release dates, patch revisions and criticality of patches;

e. Improved methodology for gathering and storing evidence. URE streamlined the means of gathering and storing evidence to demonstrate that the patch notifications are adequately monitored, are being properly tracked, and are assessed within 30 days;

f. Improved process flow for assessment. URE developed a detailed process flow to diagrammatically show how the updated process works; and

g. Enhanced security patch management program. This program was updated and re-published to reflect the improvements and enhancements discovered during the mitigation process.

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

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

FRCC201100420 (CIP-005-1 R2.2)

URE's Mitigation Plan to address its violation of CIP-005-1 R2.2 was submitted to FRCC on September 28, 2011. The Mitigation Plan was accepted by FRCC on November 28, 2011 and approved by NERC on September 10, 2012. The Mitigation Plan for this violation is designated as FRCCMIT006180 and was submitted as non-public information to FERC on September 12, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Address the lack of ports and services documentation. URE created specific documents identifying authorized ports and services on a per application basis. URE also approved access control list documents which associate all ports and services by application with each cyber asset running an application;
2. Address the lack of required documentation related to the process of access request and authorization. URE created a document addressing this issue, with section 3.2 being devoted to authorization and granting of logical and physical access;
3. Document and identify authentication methods. URE created a document addressing this issue, with Section 3.1 being devoted to authentication methods;
4. Document the review process for authorization rights; and
5. Identify dial-up controls. URE created a document outlining the controls for dial-up access.

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

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

FRCC201100421 (CIP-007-1 R2)
URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to FRCC on June 21, 2011. The Mitigation Plan was accepted by FRCC on August 11, 2011 and approved by NERC on August 23, 2012. The Mitigation Plan for this violation is designated as FRCCMIT005619 and was submitted as non-public information to FERC on August 23, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Document the process to ensure that only those ports and service required for normal and emergency operations are enabled;
2. Document the authorized ports and services for each CA class;
3. Document the test procedures by asset class to confirm implementation;
4. Run the test procedures to ensure that only those authorized ports and services are listening for connections; and

5. Identify technical infeasibilities and submit TFEs accordingly.

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

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

FRCC2011007241 (CIP-007-1 R8)
URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to FRCC on October 6, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on January 23, 2011. The Mitigation Plan for this violation is designated as FRCCMIT006203 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Conduct a vulnerability assessment;
2. Identify and document only ports and services by asset class, including ports and services testing;
3. Review controls for default accounts. URE updated procedure to identify the vulnerability assessment process, requiring a review of all security controls for default accounts; and
4. Document the results of its vulnerability assessments and include corrective actions. URE added to its documents instructions related to the assessment and corrective actions associated with any findings. Action plans from previous vulnerability assessments were also addressed as part of this Mitigation Plan.

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

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

FRCC2011007252 (CIP-005-1 R4.5)
URE's Mitigation Plan to address its violation of CIP-005-1 R4.5 was submitted to FRCC on October 6, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on December 23, 2011. The Mitigation Plan for this violation is

designated as FRCCMIT006202 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Conduct an annual CVA;
2. Document CVA identifying process. The updated document reflects all CA CVA processes; and
3. Document the results and actions plans. The updated documents cover documenting of CVA, and also include section for action plan if any differences are found in the assessment. URE created a baseline identification asset documents to identify current vulnerability state of all protected CIP assets.

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

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

FRCC2011007256 (CIP-006-1 R6)

URE's Mitigation Plan to address its violation of CIP-006-1 R6 was submitted to FRCC on September 28, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on December 23, 2011. The Mitigation Plan for this violation is designated as FRCCMIT006198 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Work with its established physical access control provider to identify standard maintenance and testing procedures for physical protection of the CIP areas;
2. Perform initial testing and maintenance procedures for establishing physical access control for all affected devices, and document the results;
3. Formally document the detailed maintenance and testing procedure;
4. Approve the documents listed above by the URE releasing authority; and
5. Re-perform testing and maintenance procedure if any changes between the initial testing and the formally approved documents exist.

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

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

FRCC2011007257 (CIP-007-1 R3)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to FRCC on October 6, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on December 23, 2011. The Mitigation Plan for this violation is designated as FRCCMIT006204 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Perform an analysis of required applications to ensure that all applicable applications are included within URE's patch management program; and
2. Update its security patch management program after the analysis is completed.

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

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

FRCC2011007259 (CIP-007-1 R5)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to FRCC on September 28, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on December 23, 2011. The Mitigation Plan for this violation is designated as FRCCMIT006199 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Address the documentation shortcoming related to R5.1 by modifying the access control scope and clearly including authorization for infrastructure assets and not just for information assets;
2. Address the shortcoming related to R5.1.3 by ensuring that the documents related to annual review of user accounts comply with this Standard;

3. Address its policy related to special accounts. URE removed accounts where possible and aligned its documentation with R5.2;
4. Identify individuals with shared account access and create an identification document containing the required information; and
5. Address the special requirements for password setting by filing TFEs for all equipment that cannot enforce these requirements.

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

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

FRCC2011007260 (CIP-007-1 R6)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to FRCC on September 28, 2011. The Mitigation Plan was accepted by FRCC on November 1, 2011 and approved by NERC on December 23, 2011. The Mitigation Plan for this violation is designated as FRCCMIT006200 and was submitted as non-public information to FERC on December 23, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Ensure that the Standard is adequately addressed in URE's documentation. URE ensured that all applicable devices are properly logging as part of its change management process;
2. Ensure that URE's logging system is searchable and information is retrievable; and
3. Replace its security status monitoring program with security status and electronic access monitoring and develop any required processes and procedures.

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

After FRCC's review of URE's submitted evidence, FRCC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[22]

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,[23] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 10, 2012. The NERC BOTCC approved the Settlement Agreement, including FRCC's assessment of a one hundred and fifty thousand dollar ($150,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE self-reported three of the violations and received self-report credit, as discussed above;
2. URE's compliance history;
3. The violation of CIP-007-1 R3 (FRCC2011007257), included in this Full NOP, is a repeat violation of FRCC201000378, which involves the same Standard and is also included in this Full NOP;
4. FRCC reported that URE was cooperative throughout the compliance enforcement process;
5. FRCC considered URE's compliance program a neutral factor in determining the penalty, as discussed above;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. FRCC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and

[22] *See* 18 C.F.R. § 39.7(d)(4).

[23] *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).

8. FRCC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and 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

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

a) Settlement Agreement by and between FRCC and URE executed July 31, 2012, included as Attachment a;

b) Record documents for FRCC200900304 CIP-004-1 R4, included as Attachment b;

   1. URE's Self Report;
   2. URE's Mitigation Plan designated as MIT-08-2551;
   3. URE's Certification of Mitigation Plan Completion;
   4. FRCC's Verification of Mitigation Plan Completion;

c) Record documents for FRCC201000312 CIP-007-1 R1, included as Attachment b;

   1. FRCC's Spot-Check Report;
   2. URE's Mitigation Plan designated as MIT-08-2478;
   3. URE's Certification of Mitigation Plan Completion;
   4. FRCC's Verification of Mitigation Plan Completion;

d) Record documents for FRCC201000377 CIP-006-2 R5, included as Attachment d;

   1. URE's Self Report;
   2. URE's Mitigation Plan designated as MIT-10-3253;
   3. URE's Certification of Mitigation Plan Completion;
   4. FRCC's Verification of Mitigation Plan Completion;

e) Record documents for FRCC201000378 CIP-007-1 R3, included as Attachment e;

1. URE's Self Report;
2. URE's Mitigation Plan designated as MIT-09-3254;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

f) Record documents for FRCC201100420 CIP-005-1 R2, included as Attachment f;

1. URE's Self-Certification;
2. URE's Mitigation Plan designated as FRCCMIT006180;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

g) Record documents for FRCC201100421 CIP-007-1 R2, included as Attachment g;

1. URE's Self-Certification;
2. URE's Mitigation Plan designated as;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

h) Record documents for FRCC2011007241 CIP-007-3 R8, included as Attachment h;

1. URE's Self-Certification;
2. URE's Mitigation Plan designated as MIT-00-6203;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

i) Record documents for FRCC2011007252 CIP-005-1 R4, included as Attachment i;

1. FRCC's Spot-Check Report;
2. URE's Mitigation Plan designated as MIT-00-6202
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

j) Record documents for FRCC2011007256 CIP-006-1 R6, included as Attachment j;

1. FRCC's Spot-Check Report;
2. URE's Mitigation Plan designated as MIT-00-6198;

3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

k) Record documents for FRCC2011007257 CIP-007-1 R3, included as Attachment k;

1. FRCC's Spot-Check Report;
2. URE's Mitigation Plan designated as MIT-00-6204;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

l) Record documents for FRCC2011007259 CIP-007-1 R5, included as Attachment l;

1. FRCC's Spot-Check Report;
2. URE's Mitigation Plan designated as MIT-00-6199;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

m) Record documents for FRCC2011007260 CIP-007-1 R6, included as Attachment m;

1. FRCC's Spot-Check Report;
2. URE's Mitigation Plan designated as MIT-00-6200;
3. URE's Certification of Mitigation Plan Completion;
4. FRCC's Verification of Mitigation Plan Completion;

A Form of Notice Suitable for Publication[24]

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

[24] *See* 18 C.F.R § 39.7(d)(6).

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile Charles.Berardesco@nerc.net Stacy Dochoda* President and Chief Executive officer Florida Reliability Coordinating Council, Inc. 1408 N. Westshore Blvd., Suite 1002 Tampa, Florida 33607-4512 (813) 289-5644 (813) 289-5646 – facsimile sdochoda@frcc.com Linda Campbell* VP and Executive Director Standards & Compliance Florida Reliability Coordinating Council, Inc. 1408 N. Westshore Blvd., Suite 1002 Tampa, Florida 33607-4512 (813) 289-5644 (813) 289-5646 – facsimile lcampbell@frcc.com	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net Barry Pagel* Director of Compliance Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 690 Tampa, Florida 33607-8402 (813) 207-7968 (813) 289-5648 – facsimile bpagel@frcc.com *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

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

cc: Unidentified Registered Entity
Florida Reliability Coordinating Council, Inc.

Attachments