PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

February 29, 2012

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. 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 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 Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations[3] of: CIP-002-1 Requirement (R) 1.1, R3.1; CIP-003-1 R1, R3, R4.2; CIP-004-1 R2, R3, R4; CIP-006-1 R1.1; CIP-007-1 R1, R4, R5.2.3; and CIP-009-1 R1.2, R5.[4] According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of forty thousand dollars ($40,000), in addition to

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

[2] *See* 18 C.F.R § 39.7(c)(2).

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

[4] At the time of the violations, Version 1 of the CIP Standards was in effect and was mandatory and enforceable for URE. CIP Version 1 became effective on June 1, 2006 and remained enforceable through March 31, 2010. CIP Version 2 was approved by the Commission and became enforceable on April 1, 2010 and was enforceable through September 30, 2010. CIP Version 3 was approved by the Commission and became enforceable on October 1, 2010. For consistency in this filing, Version 1 of the CIP Standards is used throughout.

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 SPP200900135, SPP201000222, SPP201000223, SPP201000224, SPP201000219, SPP201000225, SPP201000226, SPP201000227, SPP201000220, SPP201000228, SPP201000221, SPP201000229, SPP201000230 and SPP201000231 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 February 24, 2012, by and between SPP RE and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), 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
Southwest Power Pool Regional Entity	Unidentified Registered Entity	NOC-721	SPP200900135	CIP-002-1	1.1	Lower	$40,000
			SPP201000222	CIP-002-1	3.1	Lower	
			SPP201000223	CIP-003-1	1/1.1	Lower[5]	
			SPP201000224	CIP-003-1	3	Lower	
			SPP201000219	CIP-003-1	4.2	Lower[6]	

[5] CIP-003-1 R1 has a "Medium" Violation Risk Factor (VRF); CIP-003-1 R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective. In the context of this case, SPP RE determined the violation related to CIP-003-1 R1.1 and a "Lower" VRF was appropriate.

[6] CIP-003-1 R4 and R4.1 each have a "Medium" VRF; CIP-003-1 R4.2 and R4.3 each have a "Lower" VRF. When NERC first filed VRFs, it assigned CIP-003-1 R4 and R4.1 a "Lower" VRF.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			SPP201000225	CIP-004-1	2	Lower[7]	
			SPP201000226	CIP-004-1	3	Medium[8]	
			SPP201000227	CIP-004-1	4	Lower[9]	
			SPP201000220	CIP-006-1	1.1	Medium[10]	
			SPP201000228	CIP-007-1	1	Medium[11]	
			SPP201000221	CIP-007-1	4	Medium[12]	
			SPP201000229	CIP-007-1	5.2.3	Medium	
			SPP201000230	CIP-009-1	1.2	Medium	
			SPP201000231	CIP-009-1	5	Lower	

[7] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; CIP-004-1 R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 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-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[8] CIP-004-1 R3 has a "Medium" VRF; CIP-004-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 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 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[9] CIP-004-1 R4 and R4.1 each have a "Lower" 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.

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

[11] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; CIP-007-1 R1.2 and R1.3 each have a "Lower" VRF.

[12] When NERC filed VRFs it originally assigned CIP-007-1 R4 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-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the "Medium" VRF became effective.

SPP200900135: CIP-002-1 R1.1

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

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.…Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R1.1 provides:

> R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
>
> > R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

CIP-002-1 R1.1 has a "Lower" VRF and a "High" Violation Severity Level (VSL).[13]

During a Spot Check, SPP RE discovered URE had a violation of CIP-002-1 R1.1 because the evaluation criteria provided in URE's risk-based assessment methodology (RBAM) was too vague for identification of Critical Assets. For instance, the RBAM included the following criteria: a substation would be considered a Critical Asset if N-1 or load flow study indicated the substation was required for the reliability of the bulk power system (BPS). Stating that something is merely required for the reliability of the BPS is not specific enough to understand when a substation should be identified as a Critical Asset. In contrast, during the interview process of the Spot Check, URE stated that the evaluation criteria for the transmission substation refers to a voltage swing in excess of +/- 10% of nominal voltage as defined in the SPP Criteria. URE's documented evaluation criteria for identifying Critical Assets in its RBAM did not have that level of specificity.

[13] At the duration start time of URE's violations, CIP-002-1 – CIP-009-1 had Levels of Non-Compliance instead of VSLs. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards; the Commission approved the VSLs on March 18, 2010.

SPP RE determined the duration of the violation to be from when the Standard became mandatory and enforceable for the entity through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, URE had used a process for evaluation criteria but had failed to include the specificity in the documentation. In addition, there were no new Critical Assets identified based on the new methodology, and therefore all protective measures were in place for all Critical Assets prior to the application of the new methodology.

SPP201000222: CIP-002-1 R3.1

CIP-002-1 R3.1 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> > R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter….

CIP-002-1 R3.1 has a "Lower" VRF and a "N/A" VSL.[14]

During a Spot Check, SPP RE determined that URE was in violation of CIP-002-1 R3.1 for failing to identify and develop a complete list of Critical Cyber Assets (CCAs). Specifically, URE developed a list of its identified Critical Assets as required by CIP-002-1 R2. From that list, URE developed a list of CCAs essential to the operation of the Critical Asset; however, URE failed to include operator consoles and

[14] *See supra* n. 13.

Inter-Control Center Communications Protocol (ICCP) systems, which are essential for exchanging real-time operational data with the SPP Reliability Coordinator on the CCA list.

According to URE, the operator consoles were not listed as CCAs because it believed the redundancy of multiple operator consoles eliminated them as critical; similarly, the ICCP systems were not deemed critical because they contained backup data that was being sent to the SPP Reliability Coordinator.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through the date URE revised its CCA list to include operator consoles and ICCP systems.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to develop a complete list of CCAs, it did develop a list that included most of its CCAs. The operator consoles and ICCP systems were treated as CCAs and afforded the same protective measures as those on the CCA list. Additionally, during normal business hours (Monday – Friday, 8:00 a.m. – 4:45 p.m.), the CCAs had two layers of protection. Once inside URE's lobby, a badge was required to gain access to any area outside the lobby, including the hallway leading to the control center door, and a badge and biometrics were required to open the door to gain access to the control center. Furthermore, there were several URE operator personnel regularly working in or nearby the common area of the control center. Thus, had there been a break-in into the control center, URE operators most likely would have seen the intruder and would have investigated and/or called URE's security department prompting an immediate investigation. Even if an intruder had not been seen by an operator, the break-in would have triggered an alarm alerting URE's security department of an unauthorized access, prompting an immediate investigation. There were security cameras in the hallway monitoring access to the control center, which were monitored by security personnel during normal business hours; consequently, any malicious activity conducted during that time period would have been seen and immediately investigated by security department personnel.

Outside normal business hours, the CCAs were protected by three layers of protection. A badge and biometrics were required to gain access into the facility and such access was limited to approximately 5% of URE's overall personnel. Once inside the facility, the same two layers of protection indicated during normal business hours were in place to gain access to any of URE's CCAs. Furthermore, if an intruder had somehow gotten through all three layers of protection outside of normal business hours, times in which URE security department personnel were on-site, the break-in would have triggered an alarm alerting them of an unauthorized access prompting an immediate investigation. Also outside of normal business hours, the security cameras were under human observation; therefore, any malicious

activity conducted during that time period would have been seen and immediately investigated by security department personnel. There have been no known break-ins into any of URE's secured areas.

SPP201000223: CIP-003-1 R1

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

CIP-003-1 R1 provides in pertinent part:

> R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> > R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

CIP-003-1 R1 has a "Lower" VRF and a "Severe" VSL.[15]

During a Spot Check, SPP RE determined that URE was in violation of CIP-003-1 R1 because its cyber security policy failed to address all the requirements in Standards CIP-002 through CIP-009 and include a provision for emergency situations. Specifically, SPP RE determined that URE's cyber security policy did not identify or sufficiently identify: CIP-003-1 R2, R5; CIP-004-1 R4; CIP-005-1 R1, R2; CIP-006-1 R1, R3, R5; CIP-007-1 R1, R6, R7, R8; and CIP-009-1 R3, R4; and did not include a provision for emergency situations as required by CIP-003 R1.1.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE revised its cyber security policy.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS. Specifically, failure to address all requirements of CIP-002 through CIP-009 or include a provision for emergency situations in its cyber security policy presented a risk that all CCAs may not have had all security protections afforded them by the Standards, and despite implemented procedures for the remaining standards not identified in URE's cyber security policy, several were found to have deficiencies. The

[15] *See supra* n. 13.

risk was not serious or substantial because URE had cyber security procedures in place for all but four standards.

SPP201000224: CIP-003-1 R3

CIP-003-1 R3 provides:

> R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
>
> > R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
> >
> > R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.
> >
> > R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

CIP-003-1 R3 has a "Lower" VRF and a "Severe" VSL.[16]

During a Spot Check, SPP RE determined that URE had a violation of CIP-003-1 R3, specifically R3.2 and R3.3. Regarding R3.2, although URE's documented exceptions to its cyber security policy from a previous year included account name, date, reason and a description of the exceptions, it failed to include any compensating measures or a statement accepting risk. Regarding R3.3, URE failed to conduct an annual review and re-approval of one of its previous year's documented exceptions. The exception pertained to a password of a non-CCA server located within URE's Electronic Security Perimeter (ESP) that was incapable of being changed on a quarterly basis as required by URE's cyber security policy.

[16] *See supra* n. 13.

SPP RE determined the duration of the violation to be from the first day of URE's new annual review year, through the date URE redefined its ESP, thereby eliminating all exceptions to its cyber security policy.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did have documented exceptions to its cyber security policy, and none of URE's exceptions directly related to or reflected a deficiency in URE's security controls for Critical Assets within the ESP. Moreover, the subject server within the ESP was not a CCA. While the password of the server could not be changed quarterly as required by URE's cyber security policy, domain login requiring passwords of authorized user accounts controlled access to the server.

SPP201000219: CIP-003-1 R4.2

CIP-003-1 R4.2 provides:

> R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
>
> ****
>
> R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

CIP-003-1 R4.2 has a "Lower" VRF and a "Severe" VSL.[17]

URE submitted a Self-Report to SPP RE indicating that it was in violation of CIP-003-1 R4. Specifically, although URE had documented procedures to identify and classify CCAs and manage access to information associated with CCAs, it failed to have a procedure to classify information to be protected based on the sensitivity of the CCA information as required by R4.2.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, URE had documented procedures to identify and classify CCAs. URE

[17] *See supra* n. 13.

stored CCA information on a restricted document management system and limited access file shares. URE had documented procedures to manage access to the CCA information, including limiting access to CCAs and CCA information to only those with cleared background checks and performing quarterly reviews of access lists. Moreover, URE had protective measures to protect CCA information from unauthorized access, including: file system permissions providing access control for files and folders, user group permissions controlling access to network resources based on job functions, specific application(s) to protect, analyze, and control user accounts of the document management system environment, card swipes and bio readers for sensitive areas, locking drawers, video surveillance, port and interface security to protect devices from viruses and security breaches, and password and lockout policies.

SPP201000225: CIP-004-1 R2

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 R2 provides:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
>
> R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

CIP-004-1 R2 has a "Lower" VRF and a "High" VSL.[18]

During a Spot Check, SPP RE determined that URE was in violation of CIP-004-1 R2. Specifically, up until nine months before the Spot Check, all personnel with authorized access, regardless of whether it was physical or cyber access, received face-to-face training on URE's physical access controls. Because such training only covered physical access controls to CCAs, it was not intended to constitute compliant training for those with cyber access. URE's cyber security training consisted of URE providing three cyber security policy documents via email to affected personnel with the expectation that they would read the documents. Email read receipts indicating that the email messages were opened were used as documentation of cyber security training. SPP RE concluded, however, that this type of documentation was not sufficient to demonstrate that the cyber security policy documents were in fact read by affected personnel or to show compliance with R2.1 and R2.3. URE did implement an online training system addressing the requirements of R2.1 and R2.3 nine months prior to the Spot Check.

In a separate occurrence, two URE employees with cyber access did not receive URE's cyber security training (*i.e.*, did not receive the three cyber policy documents via email) within 90 days of receiving such access as required by R2.1. One of these individuals was granted access to operating systems but did not receive training until six months later. The other individual was granted supervisory control and data acquisition (SCADA) access but did not receive training until six months later.

Additionally, no training records could be located for four individuals with unescorted physical access. Of these individuals, one was a seasonal employee working only for a five-month period who was a certified law enforcement officer assigned to an outdoor patrol with access to URE's data center and

[18] *See supra* n. 13.

operations center for emergency situations.[19] Another employee was a certified law enforcement officer who also was assigned to an outdoor patrol with access to URE's data center and operations center for emergency situations. The other two individuals worked with the maintenance crew

Finally, for individuals with unescorted physical access, URE conducted face-to-face training over the policies, access controls and procedures covering CCAs upon receipt of their access badges; however, URE's documentation did not demonstrate that such training was repeated on an annual basis as required by R2.3.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE could not provide documentation of strict compliance for the cyber security training as required by R2.1 and R2.2, URE implemented a new compliant online training system nine months before the Spot Check; consequently, the deficiencies of URE's cyber security training for personnel with cyber access were mitigated prior to the Spot Check. Additionally, personnel risk assessments (PRAs) had been conducted for all involved personnel with cyber access. The two individuals with cyber access not receiving training within 90 days from being granted are both long-time trusted employees and both were familiar with the policies, access controls and procedures for operating CCAs.

Of the four individuals with physical access for whom no training records could be located, one was a seasoned certified law enforcement officer with government clearance (*e.g.*, cleared background check), and even though he had credentials to access the data center and operations center for emergency situations, he did not do so. A second individual was also a certified police officer with government clearance. The remaining two individuals were long-time trusted employees familiar with the policies, access controls, and procedures for operating CCAs. Finally, although documentation could not be provided showing the face-to-face training for personnel with authorized physical access was conducted annually as required by R2.3, except for the four individual for whom no training records could be located, URE has documentation showing that training had been conducted for all other affected personnel upon their receipt of access badges, and all affected personnel received training during the second half of the year of the Spot Check.

[19] The access log indicates that this individual received training; however, the training certificate could not be located.

SPP201000226: CIP-004-1 R3

CIP-004-1 R3 provides:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> > R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
> >
> > R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
> >
> > R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3 has a "Medium" VRF and a "N/A" VSL.[20]

During a Spot Check, SPP RE determined that URE was in violation of CIP-004-1 R3. Specifically, SPP RE discovered that PRAs for six employees had not been completed within thirty days of being granted unescorted physical access and/or cyber access to URE CCAs. Of those six individuals, the first one was granted physical and cyber access but the PRA was not completed until six months later. The second individual was granted physical and cyber access on but the PRA was also not completed until six months later. The third individual was granted physical access but the PRA was not completed until eleven weeks later. The fourth individual was granted physical access but the PRA was not completed until five weeks later. The fifth individual was granted physical access but the PRA was not completed

[20] *See supra* n. 13.

until six weeks later. The sixth individual was granted physical access but the PRA was not completed until five months later. The belated PRAs represented less than 5% of the overall PRAs completed by URE.

SPP RE determined the duration of the violation to be from when the Standard became mandatory and enforceable for the entity and the first individual had already been granted access without a PRA, through when URE completed the last overdue PRA.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, the six individuals represented less than 5% of the individuals on URE's approved access list. Five of the six individuals were long-time trusted employees with no performance or conduct issues. The other individual was a certified law enforcement officer with government security clearance who had a cleared background check by the state.

SPP201000227: CIP-004-1 R4

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
> >
> > R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" VRF and a "Moderate" VSL.[21]

[21] *See supra* n. 13.

During a Spot Check, SPP RE determined that URE had a violation of CIP-004-1 R4 for failing to adequately maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, the entity maintained records of personnel with electronic access to networking and communications devices and key software displays, with access rights; however, access was not documented for operating system or database user accounts. Additionally, while the documented access was being reviewed quarterly for employees, the continued need for access by key software vendor support personnel was not confirmed with the vendor.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through the date URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, only personnel with cyber security training and PRAs had access to operating system and database user accounts. Additionally, firewalls limited connectivity to the ESP to only recognized network users. Further, the operating system and database user accounts are located within a room with electronic access control and video monitoring. Although the continued need for access by the EMS/SCADA vendor support personnel was not being confirmed with the vendor, the vendor did review its access list on a quarterly basis and updated the list if the status of an individual on the list had changed. Moreover, no individual's access rights were affected during or after the completion of the Mitigation Plan, and there was no evidence that any individual gained improper access to any of URE's CCAs.

SPP201000220: CIP-006-1 R1.1

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

CIP-006-1 R1.1 provides:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security

> Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 R1.1 has a "Medium" VRF and a "High" VSL.[22]

URE submitted a Self-Report to SPP RE indicating that it was in violation of CIP-006-1 R1.1. Specifically, URE identified and documented its backup control center and data center as two distinct Physical Security Perimeters (PSPs). Both PSPs contain CCAs and reside within URE's ESP. Approximately 60 feet of network cable connecting both PSPs was installed above the ceiling tiles through metal trusses without being protected by conduit or alternate means to control physical access to the CCAs.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, although URE failed to protect the network cable in the hallway between the two ESPs, the cable was completely concealed above ceiling tiles. Furthermore, the network cable connecting the two PSPs was unmarked and installed alongside other cables not associated with the PSPs. Thus, an intruder would not have been able to visibly identify which cable connected the two ESPs. Even if the network cable had been cut and an intruder had attempted to connect to a laptop, the ports would have been disabled, thereby disallowing sensitive information to be transported to the laptop.

During normal business hours, URE's CCAs had two layers of protection. Once inside URE's lobby, a badge was required to gain access to any area outside the lobby, including the hallway where the cable is installed. Thus, had there been a break-in during normal business hours, URE operators, who work throughout areas beyond the lobby on a daily basis, most likely would have seen the intruder and would have investigated and/or called URE's security department prompting an immediate investigation. Even if an intruder had not been seen by an operator, the break-in would have triggered an alarm alerting URE's security department of an unauthorized access prompting an immediate investigation. The hallway where the cable is installed was under camera observation, which was recorded twenty-four hours a day, seven days a week, and monitored during normal business hours; consequently, any malicious activity conducted during that time period would have been seen and immediately investigated by security department personnel.

[22] *See supra* n. 13.

Outside normal business hours, the CCAs were protected by three layers of protection. A badge and biometrics were required to gain access into the facility. Once inside the facility, the same two layers of protection indicated during normal business hours were in place to gain access to any of URE's CCAs. If an intruder somehow had gotten through all three layers of protection outside of normal business hours, times in which URE security department personnel were on site, the break-in would have triggered an alarm alerting them of an unauthorized access prompting an immediate investigation. Outside of normal business hours, the security cameras were under human observation;[23] therefore, any malicious activity conducted during that time period would have been seen and immediately investigated by security department personnel. Finally, there have been no known break-ins into any of URE's ESPs.

SPP201000228: 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:

> 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.

[23] Human observation during this time was in addition to normal business hours.

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

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.[24]

During a Spot Check, SPP RE determined that URE was in violation of CIP-007-1 R1. Specifically, URE was unable to provide evidence of compliant testing from its EMS/SCADA vendor of version upgrades of operating systems, software patches and security patches; therefore, URE failed to ensure that new Critical Assets and significant changes to existing Critical Assets within its ESP did not adversely affect existing cyber security controls. SPP RE also determined that URE staff regularly transferred one or more laptop personal computers (PCs) between the protected networks within the ESP and external networks without performing the required "new CCA" testing.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to test new Critical Assets or significant changes to existing Critical Assets within URE's ESP presented a risk that the installation of an upgrade or patch would introduce exploitable vulnerabilities in URE's CCAs and/or other Critical Assets without its knowledge. Such vulnerabilities, if exploited, could result in loss of sensitive data, corruption of data, manipulation of applications or data, or complete system failure, thereby placing the reliability of the BPS at risk. URE attested that its EMS/SCADA vendor did apply security updates and functional testing of those updates was performed in an offline environment; such testing would alert URE if changes or new assets affected the operation of a Critical Asset. Some changes related to security control systems were protected by anti-virus software. The Critical Assets and CCAs within the ESP were only accessible to those with authorized physical and/or electronic access rights. The failure to test the laptops that migrated between the protected ESP and open networks as new Critical Assets presented a risk that the hardware would import compromised or a malicious program or code into the protected ESPs connected to CCAs. This risk of compromise to Critical Assets within the ESP was reduced by the isolated nature of its network without Internet connectivity.

[24] *See supra* n. 13.

SPP201000221: CIP-007-1 R4

CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
> >
> > R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.[25]

URE submitted a Self-Report to SPP RE indicating that it was in violation of CIP-007-1 R4 for failing to test anti-virus software signature files before installing them on its SCADA servers. Seven months later, URE submitted a second Self-Report stating that it failed to install the most recent anti-virus software prevention signatures on the SCADA servers as required by R4 because it did not have a test environment for evaluating anti-virus or malware prevention signatures. At the time of the violation, URE's SCADA vendor's patch management service did not support URE's version of its SCADA system. Additionally, URE failed to implement a process for updating anti-virus and malware prevention signatures as required by R4.2. SPP RE, for efficiency, agreed to incorporate the newly discovered instances of the first Self-Report into the second Self-Report.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to test anti-virus software signature files before

[25] *See supra* n. 13.

installing them increases the risk of introducing exploitable vulnerabilities in URE's CCAs and/or Critical Assets without its knowledge. Such vulnerabilities, if exploited, could have resulted in loss of sensitive data, corruption of data, manipulation of applications or data, or complete system failure, thereby placing the reliability of the BPS at risk. URE attested that its EMS/SCADA vendor did apply security updates and functional testing of those updates was performed in an offline environment; such testing would alert URE if changes or new assets affected the operation of a Critical Asset. Additionally, some changes related to security control systems were protected by anti-virus software despite URE's failure to test patch updates. Moreover, the Critical Assets and CCAs within the ESP were only accessible to those with authorized physical and/or electronic access rights. This risk of compromise to Critical Assets within the ESP was reduced by the isolated nature of its network without Internet connectivity.

SPP201000229: CIP-007-1 R5.2.3

CIP-007-1 R5.2.3 provides:

> 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.
>
> ****
>
> R5.2. 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.
>
> ****
>
> R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

CIP-007-1 R5.2.3 has a "Medium" VRF and a "Severe" VSL.[26]

During a Spot Check, SPP RE determined that URE had a violation of CIP-007-1 R5.2.3. Specifically, URE dispatchers shared an operating system user account to log into operator console workstations located in a control room within an ESP. A dispatcher voluntarily terminated his employment (retired) with URE. Although the employee's physical and network access was removed on the date of his departure, the shared user account was not changed within seven days of his departure as required by URE's policy, because the personnel responsible for changing the operator console password did not receive notification that the employee had retired.

SPP RE determined the duration of the violation to be from 24 hours after the dispatcher's final employment date as required by URE policy, through the date five months later when URE changed the shared dispatcher operator console workstation user account.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, although URE failed to change the shared user account after the dispatcher terminated his employment with URE, the dispatcher's physical and network access was removed on the date of his departure. Additionally, dispatchers did not have remote access to the operator console workstations, as the password could only be used within the secured control room located inside the ESP, and the password was available only to dispatchers authorized to access the subject control room. Therefore, the former employee was incapable of accessing the shared user account without first gaining entry into the control room. Moreover, URE's EMS/SCADA vendors did not have access to the subject user account password.

SPP201000230: CIP-009-1 R1.2

The purpose statement of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-009-1 R1.2 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

[26] *See supra* n. 13.

****

R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R1.2 has a "Medium" VRF and a "High" VSL.[27]

During a Spot Check, SPP RE determined that URE had a violation of CIP-009-1 R1.2. Specifically, although URE's CCA recovery plan included the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan as required by R1.1, it did not define the roles and responsibilities of incident responders.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, while not as comprehensive as required by the Standard, URE did have a recovery procedure in place, and the entity support staff are very experienced in the support of CCAs and reasonably expected to have been able to perform the appropriate recovery steps for a wide variety of incidents. Additionally, URE's communications policies and procedures had a callout progression list with contact names and numbers and defined roles and responsibilities covering various events.

SPP201000231: CIP-009-1 R5

CIP-009-1 R5 provides in pertinent part: "Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

CIP-009-1 R5 has a "Lower" VRF and a "Severe" VSL.[28]

During a Spot Check, SPP RE determined that URE had a violation of CIP-009-1 R5. Specifically, although URE stored information essential to the restoration of a failed or compromised CCA daily on backup media, the backup media was not tested to verify all essential information was available.

[27] *See supra* n. 13.
[28] *See supra* n. 13.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable for the entity, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, although tests were not conducted to verify all essential information was available, URE did use software that automatically ran backups of its CCAs, and reports of such backups were regularly reviewed to ensure that backups were running as scheduled and that were no reported errors. Moreover, URE has not had any incidents in the past requiring recovery of CCAs from a backup.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of forty thousand dollars ($40,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors: (1) The violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards; (2) URE self-reported three of the violations;[29] (3) URE was cooperative throughout the compliance enforcement process; (4) There was no evidence of any attempt to conceal a violation nor evidence of intent to do so; (5) The violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and (6) URE had a compliance program in effect at the time of the violations which SPP RE considered a mitigating factor in the penalty determination.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of forty thousand dollars ($40,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[30]

SPP200900135: CIP-002-1 R1.1

URE's Mitigation Plan to address its violation of CIP-002-1 R1.1 was submitted to SPP RE on October 21, 2009. The Mitigation Plan was accepted by SPP RE on January 20, 2010 and approved by NERC on January 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2297 and was submitted as non-public information to FERC on January 27, 2010 in accordance with FERC orders.

[29] URE submitted Self-Reports for SPP201000219 CIP-003-1 R4.2, SPP201000220 CIP-006-1 R1.1 and SPP201000221 CIP-007-1 R4.
[30] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. Revise its RBAM document to include the evaluation criteria required by CIP-002-1 R1.1. The revised methodology will be used to identify Critical Assets for which URE is responsible.
2. Develop this methodology using a standardized process addressing the following asset categories:
    a. Control centers and backup control centers;
    b. Substations that support the reliable operation of the BPS;
    c. Resources that support the reliable operation of the BPS;
    d. Systems and facilities critical to system restoration;
    e. Systems and facilities critical to automatic load shedding;
    f. Special protection systems that support the reliable operation of the BPS; and
    g. Any additional assets that support the reliable operation of the BPS.
3. Document evaluation criteria for each of the aforementioned asset categories to determine whether a URE asset is a Critical Asset.

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

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

SPP201000222: CIP-002-1 R3.1

URE's Mitigation Plan to address its violation of CIP-002-1 R3.1 was submitted to SPP RE on July 26, 2010. The Mitigation Plan was accepted by SPP RE on August 2, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2741 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE's Mitigation Plan stated that URE had updated the CCA list to include the system operator consoles and ICCP system, and as an additional precaution, URE installed lock boxes to secure the operator consoles/personal computer hardware located in a control center.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its revised CCA list identifying operator consoles and ICCP systems as CCAs.

After SPP RE's review of URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed on March 3, 2010.

SPP201000223: CIP-003-1 R1

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted to SPP RE on July 29, 2010. The Mitigation Plan was accepted by SPP RE on August 3, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2742 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE's Mitigation Plan stated URE had revised its cyber security plan to include all provisions of CIP-002 through CIP-009 and included a provision for emergency situations.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its revised cyber security policy.

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

SPP201000224: CIP-003-1 R3

URE's Mitigation Plan to address its violation of CIP-003-1 R3 was submitted to SPP RE on July 23, 2010. The Mitigation Plan was accepted by SPP RE on August 3, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2743 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. Conducted a review of its previous year's documented exceptions to its cyber security policy;
2. Determined that only one exception remained—the password of a non-CCA server could not be changed on a quarterly basis as required by URE's cyber security policy;
3. Revised its exception list to include the sole exception and included compensating measures, which was approved by the authorized senior manager; and

4. URE and SPP RE discussed whether a Technical Feasible Exception (TFE) needed to be filed to address the documented exception but concluded the TFE was unnecessary and instead, URE redefined its ESP. Consequently, the server is no longer within the ESP and has been removed from the exception list. URE has no documented exceptions to its cyber security policy.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its revised cyber security policy exceptions document.

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

SPP201000219: CIP-003-1 R4.2

URE's Mitigation Plan to address its violation of CIP-003-1 R4.2 was submitted to SPP RE on October 14, 2010. The Mitigation Plan was accepted by SPP RE on October 27, 2010 and approved by NERC on November 17, 2010. The Mitigation Plan for this violation is designated as MIT-08-3013 and was submitted as non-public information to FERC on November 19, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop and document an information protection program as required by CIP-003 R4. URE will train;
2. Train appropriate staff on the program;
3. As part of the program, URE will begin implementation to identify, classify and protect information associated with CCAs;
4. Implement an application for its document management system security and permission management for protected information; and
5. At least annually, assess adherence to the program, document the assessment results, and implement an action plan to remediate any deficiencies identified during the assessment.

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

1. URE's CCA information protection program document;
2. URE's data classification policy;
3. URE's training program presentation and logs; and

4. Several URE staff attestations of compliance with the Standard.

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

SPP201000225: CIP-004-1 R2

URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted to SPP RE on July 23, 2010. The Mitigation Plan was accepted by SPP RE on August 3, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2744 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. For people who have electronic access to CCAs, URE moved to an online training system. This system follows the progress of the employee from the time the employee is registered on the system through completion of the test at the end of the training course.
2. For people who have physical access only to CCAs, the URE security department met with employees and trained them using a presentation. Attendees signed in to verify they had been trained.
3. Training is now required to be completed before the employee/contractor is given unescorted physical access or electronic access to CCAs.
4. For existing employees, they are required to complete the training each year before the end of the month of June or their access (electronic and/or physical) is terminated. URE has begun scheduling to make sure that all required employees are trained by the end of June each year.

URE certified on that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's security department cyber security training presentation document on proper access control use and log sheet;
2. URE's email notification of required online cyber security training for personnel with cyber access;
3. URE's quarterly review of authorized access list; and
4. URE's revised training process document.

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

SPP201000226: CIP-004-1 R3

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to SPP RE on July 22, 2010. The Mitigation Plan was accepted by SPP RE on August 3, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation is designated as MIT-08-2745 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE had already mitigated the violation prior to the Spot Check by conducting PRAs for the affected personnel. To prevent recurrence of the violation, URE revised its PRA policy to require PRAs to be completed prior to authorizing cyber and unescorted physical access to CCAs. URE also implemented a work flow system to verify the progress of each person through the background investigation process. The workflow now requires the URE security department to inform the individual (*e.g.*, supervisor) requesting the PRA when the process has been completed, ensuring that no one is inadvertently omitted from having a completed PRA.

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

1. URE's personnel access list;
2. An email with attached new PRA workflow procedures; and
3. URE's revised PRA policy**.**

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

SPP201000227: CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SPP RE on June 30, 2010. The Mitigation Plan was accepted by SPP RE on July 12, 2010 and approved by NERC on August 11, 2010. The Mitigation Plan for this violation is designated as MIT-08-2662 and was submitted as non-public information to FERC on August 12, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. URE revised its CCA access review procedures to include a documented review of its operating system and database user accounts. Specifically, URE added columns to its spreadsheet used to

track personnel and training and included a column describing access to all CCAs, including key software;

2. URE requested and received from its EMS/SCADA vendor the most current access list of support personnel and details of each individual's PRA and written confirmation of the continued need for access by its support personnel;
3. URE also requested and received from its EMS/SCADA vendor written confirmation that it would update its access list and provide it to URE within 24 hours of employee termination for cause, or seven days for personnel who no longer requires access to URE's CCAs; and
4. URE disabled the EMS/SCADA vendor from its shared user account and will manually enable access on an as-needed basis.

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

1. URE's revised CCA access list;
2. URE email confirmation that EMS/SCADA vendor access was disabled;
3. EMS/SCADA vendor support personnel access list with PRA details;
4. EMS/SCADA vendor email confirmation that support the personnel access list is relevant for continued need for access; and
5. EMS/SCADA vendor letter referencing support personnel completed PRAs and notification it will advise URE of any personnel changes to the access list.

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

SPP201000220: CIP-006-1 R1.1

URE's Mitigation Plan to address its violation of CIP-006-1 R1.1 was submitted to SPP RE on July 26, 2010. The Mitigation Plan was accepted by SPP RE on August 5, 2010 and approved by NERC on August 30, 2010. The Mitigation Plan for this violation is designated as MIT-08-2757 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE's Mitigation Plan stated URE had protected the network cable connecting the PSPs by installing a three-inch conduit around the wiring.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following: URE's email attestations of the conduit installation.

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

SPP201000228: CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to SPP RE on November 2, 2010. The Mitigation Plan was accepted by SPP RE on November 22, 2010 and approved by NERC on December 7, 2010. The Mitigation Plan for this violation is designated as MIT-08-3109 and was submitted as non-public information to FERC on December 7, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement a reliability process manual to address testing procedures to ensure that new CCAs and significant changes to existing Critical Assets within the ESP do not adversely affect existing cyber security controls. The manual includes a detailed step-by-step process for testing procedures;
2. Purchase new hardware equipment in order to test version upgrades of URE's operating system and patches prior to their application to the production system; and
3. Purchase dedicated laptop PCs to be used only within the ESP.

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

1. URE's reliability process manual document;
2. URE's laptop PCs purchase order;
3. URE's master patch update list; and
4. URE's attestation of compliance with the Standard.

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

SPP201000221: CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to SPP RE on July 29, 2010. The Mitigation Plan was accepted by SPP RE on August 10, 2010 and approved by NERC on August 30, 2010. The Mitigation Plan for this violation is designated as MIT-08-2758 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. Documented and implemented a systems management process for updating anti-virus and malware preventative signatures. The process has detailed procedures for testing and installing the signature files. URE now tests all anti-virus software and malware preventative signatures before installing them on its SCADA servers; and
2. Upgraded its SCADA system, which is now supported by URE's SCADA vendor's patch management service.

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

1. URE's systems management process policy document;
2. URE's email attestation of pre-set calendar reminders for checking system protection measure updates;
3. URE's log of security updates to SCADA servers; and
4. URE's procedure document for testing updates of anti-virus and malware prevention signatures.

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

SPP201000229: CIP-007-1 R5.2.3

URE's Mitigation Plan to address its violation of CIP-007-1 R5.2.3 was submitted to SPP RE on June 30, 2010. The Mitigation Plan was accepted by SPP RE on July 20, 2010 and approved by NERC on August 19, 2010. The Mitigation Plan for this violation is designated as MIT-08-2687 and was submitted as non-public information to FERC on August 20, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. Changed the dispatcher shared operator console workstation user account password;

2. To prevent reoccurrence of the violation, the personnel responsible for changing the workstation password have been added to the notification distribution list of terminated employees; and
3. URE reduced the number of workstations with shared user account access.

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

1. URE's attestation of the changed dispatcher shared operator workstation user account; and
2. URE's attestation that personnel responsible for changing the operator console password has been added to the notification distribution list of terminated employees.

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

SPP201000230: CIP-009-1 R1.2

URE's Mitigation Plan to address its violation of CIP-009-1 R1.2 was submitted to SPP RE on August 4, 2010. The Mitigation Plan was accepted by SPP RE on August 10, 2010 and approved by NERC on August 30, 2010. The Mitigation Plan for this violation is designated as MIT-08-2759 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE took the following actions to mitigate the issue and prevent recurrence:

1. Revised its CCA recovery plan to include defined roles and responsibilities of incident responders;
2. Copied the callout progression list from URE's communications policies and procedures into a stand-alone policy; and
3. Affected support personnel for the recovery of CCAs received training on their defined roles and responsibilities.

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

1. URE's new stand-alone policy; and
2. URE's updated CCA recovery plan;

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

SPP201000231: CIP-009-1 R5

URE's Mitigation Plan to address its violation of CIP-009-1 R5 was submitted to SPP RE on July 26, 2010. The Mitigation Plan was accepted by SPP RE on August 10, 2010 and approved by NERC on August 30, 2010. The Mitigation Plan for this violation is designated as MIT-08-2760 and was submitted as non-public information to FERC on August 31, 2010 in accordance with FERC orders.

URE's Mitigation Plan stated URE had implemented a formal procedure for annually testing backup media. URE subsequently executed a backup media test and verified that all critical information essential to the restoration of a failed or compromised CCA was available.

URE certified on that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's backup tape recovery procedure document;
2. URE's staff notes confirming that tape recovery review was conducted;
3. URE's backup tape recovery verification document; and
4. URE's recovery operations process document.

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[31]

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,[32] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 7, 2012.

[31] *See* 18 C.F.R. § 39.7(d)(4).
[32] *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).

The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of a forty thousand dollar ($40,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported three of the violations;[33]
3. SPP RE reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SPP RE considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SPP RE determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. SPP RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of forty thousand dollars ($40,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure

[33] URE submitted Self-Reports for SPP201000219 CIP-003-1 R4.2, SPP201000220 CIP-006-1 R1.1 and SPP201000221 CIP-007-1 R4.

including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between SPP RE and URE executed February 24, 2012, included as Attachment a;
   1. Disposition of Violation: Information Common to Instant Violations, included as Attachment 1 to the Settlement Agreement;
   2. Disposition of Violation for CIP-002-1 R1.1, included as Attachment 1.a to the Settlement Agreement;
   3. Disposition of Violation for CIP-003-1 R4.2, included as Attachment 1.b to the Settlement Agreement;
   4. Disposition of Violation for CIP-006-1 R1.1, included as Attachment 1.c to the Settlement Agreement;
   5. Disposition of Violation for CIP-007-1 R4, included as Attachment 1.d to the Settlement Agreement;
   6. Disposition of Violation for CIP-002-1 R3.1, included as Attachment 1.e to the Settlement Agreement;
   7. Disposition of Violation for CIP-003-1 R1, included as Attachment 1.f to the Settlement Agreement;

8. Disposition of Violation for CIP-003-1 R3, included as Attachment 1.g to the Settlement Agreement;
9. Disposition of Violation for CIP-004-1 R2, included as Attachment 1.h to the Settlement Agreement;
10. Disposition of Violation for CIP-004-1 R3, included as Attachment 1.i to the Settlement Agreement;
11. Disposition of Violation for CIP-004-1 R4, included as Attachment 1.j to the Settlement Agreement;
12. Disposition of Violation for CIP-007-1 R1, included as Attachment 1.k to the Settlement Agreement;
13. Disposition of Violation for CIP-007-1 R5.2.3, included as Attachment 1.l to the Settlement Agreement;
14. Disposition of Violation for CIP-009-1 R1.2, included as Attachment 1.m to the Settlement Agreement; and
15. Disposition of Violation for CIP-009-1 R5, included as Attachment 1.n to the Settlement Agreement.

b) Record documents for the violation of CIP-002-1 R1.1, included as Attachment b:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

c) Record documents for the violation of CIP-002-1 R3.1, included as Attachment c:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

d) Record documents for the violation of CIP-003-1 R1, included as Attachment d:

1. URE's Source Document;

2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

e) Record documents for the violation of CIP-003-1 R3, included as Attachment e:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

f) Record documents for the violation of CIP-003-1 R4.2, included as Attachment f:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion dated March 22, 2011.

g) Record documents for the violation of CIP-004-1 R2, included as Attachment g:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

h) Record documents for the violation of CIP-004-1 R3, included as Attachment h:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

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

1. URE's Source Document;
2. URE's Mitigation Plan;

3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

j) Record documents for the violation of CIP-006-1 R1.1, included as Attachment j:
   1. URE's Source Document;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

k) Record documents for the violation of CIP-007-1 R1, included as Attachment k:
   1. URE's Source Document;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

l) Record documents for the violation of CIP-007-1 R4, included as Attachment l:
   1. URE's Source Document;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

m) Record documents for the violation of CIP-007-1 R5.2.3, included as Attachment m:
   1. URE's Source Document;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

n) Record documents for the violation of CIP-009-1 R1.2, included as Attachment n:
   1. URE's Source Document;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion; and

4. SPP RE's Verification of Mitigation Plan Completion.

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

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[34]

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

[34] *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 30326-1001 (404) 446-2560 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 david.cook@nerc.net Machelle Smith* Paralegal & SPP RE File Clerk Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1681 (501) 821-8726 – facsimile Spprefileclerk.re@spp.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.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net sonia.mendonca@nerc.net Stacy Dochoda* General Manager Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1730 (501) 821-8726 – facsimile Sdochoda.re@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 16101 La Grande, Ste 103 Little Rock, AR 72223 (501) 688-1672 (501) 821-8726 – facsimile Jgertsch.re@spp.org

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001
(404) 446-2560

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
david.cook@nerc.net

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

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments