PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

January 31, 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 WECC and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of BAL-005-0 R17, CIP-002-1 R1, CIP-002-1 R3, FAC-009-1 R1, PER-001-0 R1, PRC-005-1 R2, PRC-008-0 R2, PRC-011-0 R2, TOP-002-2 R19, TOP-005-1 R1, CIP-003-1 R5, CIP-004-1 R4, CIP-005-1 R2, CIP-006-2 R1, CIP-006-1 R2, CIP-006-2 R2, CIP-007-1 R2, CIP-007-1 R3, CIP-007-1 R5 and CIP-007-1 R6. According to the Settlement Agreement, URE agrees and stipulates to the facts of the violations and has agreed to the assessed penalty of one hundred thirty-five thousand dollars ($135,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (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.

the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201001853, WECC201001880, WECC201001881, WECC201001819, WECC201001824, WECC201001848, WECC201001849, WECC201001850, WECC201001823, WECC201001826, WECC200902072, WECC200902070, WECC201002084, WECC201002119, WECC201002089, WECC201002113, WECC201002060, WECC201002067, WECC201002061 and WECC201002066 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 August 25, 2011, by and between WECC 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 (2007), 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 ($)
WECC	Unidentified Registered Entity	NOC-976	WECC201001853	BAL-005-0[4]	17	Medium[5]	135,000
			WECC201001880	CIP-002-1	1	Medium[6]	

[4] The Settlement Agreement incorrectly lists the Reliability Standard as BAL-005-1. BAL-005-0 was enforceable from June 18, 2007 through August 27, 2008. BAL-005-0b was approved by the Commission and became enforceable on August 28, 2008. BAL-005-0.1b is the current enforceable Standard as of May 13, 2009. The subsequent interpretations provide clarity regarding the responsibilities of a registered entity and do not change the meaning or language of the original NERC Reliability Standard and its requirements. For consistency in this filing, the original NERC Reliability Standard, BAL-005-0, is used throughout.

[5] When NERC filed Violation Risk Factors (VRFs), it originally assigned BAL-005-0 R17 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 6, 2008, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for BAL-005-0 R17 was in effect from June 18, 2007 until February 6, 2008 when the "Medium" VRF became effective.

[6] When NERC filed VRFs, it originally assigned CIP-002-1 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-002-1 R1 was in effect from June 18, 2007 until January 27, 2009 when the "Medium" VRF became effective.

			WECC201001881	CIP-002-1[7]	3	High[8]	
			WECC201001819	FAC-009-1	1	Medium	
			WECC201001824	PER-001-0[9]	1	High	
			WECC201001848	PRC-005-1	2	High[10]	
			WECC201001849	PRC-008-0	2	Medium	
			WECC201001850	PRC-011-0	2	Lower	
			WECC201001823	TOP-002-2[11]	19	Medium	
			WECC201001826	TOP-005-1[12]	1	Medium	
			WECC200902072	CIP-003-1	5	Lower	

[7] The Settlement Agreement incorrectly lists the Reliability Standard as CIP-002-0 on page 1 of the Settlement Agreement but refers to the Standard correctly thereafter.

[8] When NERC filed VRFs, it originally assigned CIP-002-1 R3 a "Medium" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Medium" VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.

[9] PER-001-0 was enforceable June 18, 2007 through December 9, 2009. PER-001-0.1 was approved by the Commission and became enforceable on December 10, 2009.

[10] PRC-005-1 R2 has a "Lower" VRF; PRC-005-1 R2.1 and R2.2 each have a "High" VRF. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these included PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a "High" VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 "High" VRF as filed. Therefore, the "High" VRF was in effect from June 26, 2007. In the context of this case, WECC determined that the violation related to both R2.1 and R2.2, and therefore a "High" VRF is appropriate.

[11] The Settlement Agreement incorrectly refers to the Reliability Standard as TOP-002-0. TOP-002-0 was in effect from April 1, 2005 through December 31, 2006, before the instant violation's start duration date. TOP-002-2 was in effect from January 1, 2007 through December 1, 2009 and TOP-002-2a has been in effect since December 2, 2009. For consistency, this document uses TOP-002-2 throughout.

[12] TOP-005-1 was enforceable from June 18, 2007 through May 12, 2009 when it was replaced with TOP-005-1.1. TOP-005-1.1 was enforceable from May 13, 2009 through May 25, 2011 when it was replaced with TOP-005-1.1a. TOP-005-1.1a was enforceable from May 26, 2011 through September 30, 2011 when it was replaced with the current version, TOP-005-2a. TOP-005-2a was approved by the Commission and became enforceable on October 1, 2011.

			WECC200902070	CIP-004-1	4	Medium[13]	
			WECC201002084	CIP-005-1	2	Medium[14]	
			WECC201002119	CIP-006-2	1	Medium	
			WECC201002089	CIP-006-1	2	Medium	
			WECC201002113	CIP-006-2	2	Medium	
			WECC201002060	CIP-007-1	2	Medium	
			WECC201002067	CIP-007-1	3	Lower	
			WECC201002061	CIP-007-1	5	Lower	
			WECC201002066	CIP-007-1	6	Medium	

WECC201001853 BAL-005-0 R17

The purpose statement of Reliability Standard BAL-005-0 provides:

> This standard establishes requirements for Balancing Authority Automatic Generation Control (AGC) necessary to calculate Area Control Error (ACE) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area so that balancing of resources and demand can be achieved.

BAL-005-0 R17 provides:

> Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

[13] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; CIP-004-1 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.

[14] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; CIP-005-1 R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

BAL-005-0 R17 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE reported a violation of BAL-005-1 R17 through both the Self-Report and Self-Certification process.[15] URE reported that during an internal review, URE discovered it was not performing an annual check and calibration on all of its time error and frequency devices against a common reference. URE stated in its Self-Report that it has a number of total frequency source devices available for use in the Energy Management System (EMS) ACE calculation and thus in the BA's AGC. 44% of URE's time error and frequency devices are digital and the remaining 56% of the devices are analog devices. URE reported that the analog devices had not been annually checked or calibrated to a common source. WECC determined that URE had a violation of BAL-005-0 R17 because it failed to check and calibrate 44% of its digital time error and frequency devices against a common reference.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although URE failed to demonstrate it had performed a calibration check of its frequency devices' output against a calibrated frequency source, it does have telemetry which receives the time error broadcast by the Interconnection Time Monitor and has an alarm established if the time error calculated by its frequency devices and the time error distributed by the Interconnection Time Monitor deviate by 5 seconds. Thus, if the device were operating at the limit of specified accuracy of ±0.001 Hz, this alarm would actuate in approximately 83 hours, alerting URE of a problem sooner than would an annual calibration check. Furthermore, URE stated it was able to demonstrate that its devices were within the required accuracy requirements of BAL-005-1 R17 by using historical data. Based on this, WECC determined this violation posed minimal risk to the BPS.

WECC201001880 CIP-002-1 R1

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated

[15] WECC had previously notified URE that it was required to submit a Self-Certification. Since both reports were filed during the Self-Certification submittal period, WECC determined the discovery method is Self-Certification.

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 provides:

> Critical Asset Identification Method — The Responsible Entity[16] 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.
> >
> > R1.2. The risk-based assessment shall consider the following assets:
> >
> > > R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
> > >
> > > R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.
> > >
> > > R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.
> > >
> > > R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.
> > >
> > > R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.
> > >
> > > R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

[16] Within the text of Standards CIP-002-CIP-009, "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.

> R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

(Footnote added.)

CIP-002-1 R1 has a "Medium" VRF and a "N/A" VSL.[17]

WECC conducted a CIP Spot Check of URE. The WECC Spot Check team (Spot Check team) determined that evaluation criteria used in URE's risk-based assessment methodology (RBAM) included subjective evaluation criteria that could lead to the misidentification of Critical Assets. The Standard requires URE to "maintain documentation describing its risk based assessment methodology [RBAM] that includes procedures and evaluation criteria." URE's RBAM used a traditional and widely accepted risk calculation where "Risk = function (consequence x threat x vulnerability)." In this formula, URE included factors such as personnel loss, customer confidence, and environmental impact that WECC concluded are unrelated to the measurement of the criticality of the asset with regard to the BPS. Furthermore, the URE RBAM considered the likelihood of threats, rather than a measurement of the impact of a loss of a Critical Asset.

URE's RBAM was inconsistent with the September 2009 NERC Security Guideline which recommends using an impact analysis, rather than a traditional risk assessment when approaching Critical Asset identification. In the impact analysis recommended by NERC, the potential for threats and vulnerabilities always exists (*i.e.*, the probability of occurrence = 1.0).[18] As a result, WECC concluded the RBAM used by URE to identify its Critical Assets might fail to identify all Critical Assets. NERC had not provided any interpretive guidance in relation to RBAMs before September 2009. Once NERC issued its Security Guideline in September 2009, URE modified its RBAM. WECC determined that URE had a violation of CIP-002-1 R1 because the URE RBAM could result in a failure to identify all of the Critical Assets essential to the reliability and operability of the BPS.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE revised its RBAM to incorporate NERC recommendations.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because while URE considered factors in its RBAM which WECC concluded do not relate to the true criticality of the asset, the removal of these evaluation criteria results in the

[17] At the time of the violations, no VSLs were in effect for Version 1 of the CIP Reliability Standards. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

[18] North American Electric Reliability Corporation, *Security Guideline for the Electricity Sector: Identifying Critical Assets, Version 1.0*, September 17, 2009.

same Critical Asset identification as the original URE RBAM. Furthermore, URE's current RBAM has been modified to remove the possibility of this set of criteria from affecting the identification of Critical Assets. For these reasons, WECC determined this violation posed minimal risk to the BPS.

WECC201001881 CIP-002-1 R3

CIP-002-1 R3 provides:

> 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; or,
> >
> > R3.2. The Cyber Asset uses a routable protocol within a control center; or,
> >
> > R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 has a "High" VRF and a "N/A" VSL.[19]

During the CIP Spot Check, the Spot Check team concluded that URE failed to develop and review a list of Critical Cyber Assets (CCAs) essential to the operation of its identified Critical Assets. As part of the Spot Check, URE submitted its first CCA list which identified an integrated control system as URE's CCA. URE also produced a diagram that included all of the component parts constituting the integrated control system, but that diagram was not labeled as CCAs. URE submitted its second CCA list dated one year later, that contained a labeled component-by-component list of all the elements of the integrated control system identified as its CCA. WECC determined that URE had a violation of CIP-002-1 R3 because it failed to develop a labeled document listing the individual components associated with its identified CCAs until the effective date of its second CCA list.

[19] *See supra* n. 17.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE developed a labeled document listing the individual components associated with its identified CCAs.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because although URE did not have a component-by-component list labeled as CCAs, it did have diagrams that showed all assets that were included in URE's identified CCA system. For these reasons, WECC determined this violation posed minimal risk to the BPS.

WECC201001819 FAC-009-1 R1

The purpose statement of FAC-009-1 provides: "To ensure that Facility Ratings used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies."

FAC-009-1 R1 provides: "The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology."

FAC-009-1 R1 has a "Medium" VRF and a "Lower" VSL.

URE submitted both a Self-Report and Self-Certification reporting a possible violation of FAC-009-1 R1.[20] URE reported that during an internal compliance review, it had discovered a violation of FAC-009-1 R1 because it had established Facility Ratings that were inconsistent with the associated Facility Rating Methodology. URE reported that 26.5% of its facilities were given Facility Ratings that were higher than Facility Ratings determined by using URE's Facility Rating Methodology. WECC determined that URE had a violation of FAC-009-1 R1 because it established Facility Ratings that were not consistent with the associated Facility Ratings Methodology.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE established Facility Ratings for 26.5% of its equipment at a different level than the level determined by using the URE Facility Ratings Methodology, however in this case the risk was mitigated due to the limited nature of the violation, URE had used industry standards and practices to rate its facilities, and URE's system had performed successfully with the ratings in place.

[20] *See supra* n. 15.

WECC201001824 PER-001-0 R1

The purpose statement of PER-001-0 provides: "Transmission Operator and Balancing Authority operating personnel must have the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System."

PER-001-0 R1 provides: "Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System."

PER-001-0 R1 has a "High" VRF and a "High" VSL.

URE submitted both a Self-Report and Self-Certification reporting a possible violation of PER-001-0 R1.[21] URE discovered during an internal compliance review that its then-in-force job description did not contain elements specified in Measure 1 of the Standard.[22] URE reported that the current real time energy trader job description failed to state that the real time energy traders have the authority and responsibility to take or direct timely and appropriate real-time actions to ensure the stable and reliable operation of the BPS. WECC determined that URE had a violation of PER-001-0 R1 because even though URE real time energy traders did actually have all of the responsibilities and authorities required as evidenced by information provided to the subject matter expert (SME), URE failed to provide a job description that states, in clear and unambiguous language in conformance with Measure 1 of the Standard, that the real time

[21] *See supra* n. 15.

[22] Measure 1 of PER-001-0 states:

> The Transmission Operator and Balancing Authority provide documentation that operating personnel have the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System. These responsibilities and authorities are understood by the operating personnel. Documentation shall include:
>
> > M1.1 A written current job description that states in clear and unambiguous language the responsibilities and authorities of each operating position of a Transmission Operator and Balancing Authority. The position description identifies personnel subject to the authority of the Transmission Operator and Balancing Authority.
> >
> > M1.2 The current job description is readily accessible in the control room environment to all operating personnel.
> >
> > M1.3 A written current job description that states operating personnel are responsible for complying with the NERC reliability standards.
> >
> > M1.4 Written operating procedures that state that, during normal and emergency conditions, operating personnel have the authority to take or direct timely and appropriate real-time actions. Such actions shall include shedding of firm load to prevent or alleviate System Operating Limit Interconnection or Reliability Operating Limit violations. These actions are performed without obtaining approval from higher-level personnel within the Transmission Operator or Balancing Authority.

energy trader operating positions have the responsibility and authority to implement real-time actions.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS based on a statement from URE and notes from a previous compliance audit; the real time energy traders had all the authority to take real-time actions. This violation is primarily a documentation-related violation with limited potential impact to the BPS because URE failed to update job descriptions with a clear and unambiguous statement defining the position's responsibility and authority. Additionally, real time energy trader system operators are seldom in a position to respond to an emergency. For this reason, WECC determined this violation posed minimal risk to the BPS.

WECC201001848 PRC-005-1 R2

The purpose statement of PRC-005-1 provides: "To ensure all transmission and generation Protection Systems affecting the reliability of the Bulk Electric System (BES) are maintained and tested."

PRC-005-1 R2 provides:

> Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System[23] shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization[24] on request (within 30 calendar days). The documentation of the program implementation shall include:
>
> > R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.
> >
> > R2.2. Date each Protection System device was last tested/maintained.

(Footnotes added.)

PRC-005-1 R2 has a "High" VRF and a "Severe" VSL.

[23] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

[24] Consistent with applicable FERC precedent, the term "Regional Reliability Organization" in this context refers to WECC.

URE reported a violation of PRC-005-1 R2 through both the Self-Report and Self-Certification process, respectively.[25] During an internal review, URE discovered it was behind schedule for many devices covered by PRC-005-1 R2. URE stated in its Self-Report that it found maintenance and testing was not being performed on Protection System devices according to the intervals found in its transmission, generation and distribution maintenance and testing program (URE Program). Specifically, URE stated that it was behind schedule on maintenance and testing for relays, communication devices, batteries, current transformers (CTs), potential transformers (PTs) and DC circuitry. WECC determined that URE had a violation of PRC-005-1 R2 because URE was behind schedule on maintenance and testing for 19% of its protective relays. URE was also not current with maintenance and testing on 6% of its communications devices. In addition, testing and maintenance was missed, incomplete, or behind schedule on 444 monthly, 181 quarterly, 102 annual, and 53 quarter-life capacity tests maintenance intervals on 100% of its batteries. Finally, URE could provide no evidence that maintenance and testing was performed on its CTs, PTs and DC circuitry according to the URE Program. Therefore, URE was not able to demonstrate these devices were maintained or tested within the defined interval.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS. Specifically, the number of Protection System devices that are not maintained and tested on schedule increases the likelihood of a protective device failure. Due to URE's failure to maintain and test a number of devices within the defined intervals, as well as URE's failure to document the date each URE Protection System was last maintained and tested, WECC determined this violation posed moderate risk to the BPS. This violation did not pose a serious or substantial risk to the BPS because URE tested the majority of its relays pursuant to the URE Program. While URE did miss 100% of its batteries throughout the violation period, the majority of the battery inspections that URE missed were URE's monthly and quarterly tests. The URE Program includes monthly, quarterly and annual inspections with regard to its batteries.

WECC201001849 PRC-008-0 R2

The purpose statement of PRC-008-0 provides: "Provide last resort system preservation measures by implementing an Under Frequency Load Shedding (UFLS) program."

[25] URE submitted its Self-Certification and 42 days later, URE resubmitted a Self-Report for this violation. WECC had previously notified URE that it was required to submit a Self-Certification. Since the Self-Certification and first Self-Report were filed during the Self-Certification submittal period, WECC determined the discovery method is Self-Certification.

PRC-008-0 R2 provides:

> The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).

PRC-008-0 R2 has a "Medium" VRF and a "Severe" VSL.

URE reported a violation of PRC-008-0 R2 through both the Self-Report and Self-Certification process, respectively.[26] URE reported that, during an internal review, it discovered its UFLS equipment had not been completely maintained according to the intervals found in the URE Program. One relay was one day overdue and two relays were four days overdue. None of the relays were behind schedule with URE's newly set intervals. URE also stated in the Self-Report that UFLS maintenance and testing program results for its PT and DC circuitry were not documented, and therefore not available as required by the Standard. Specifically, URE reported that 88 monthly inspections, 43 quarterly inspections, 23 annual inspections and 7 quarterly life capacity tests were incomplete, behind schedule, or missed on a number of its UFLS equipment batteries. The SME also confirmed that maintenance on 12% of its UFLS devices were incomplete, behind schedule, or missed, and that URE had no maintenance and testing results available for DC circuitry. WECC determined that URE had a violation of PRC-008-0 R2 because URE failed to completely implement its UFLS program and failed to provide WECC with UFLS maintenance and testing program results required by the Standard.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS because while UFLS equipment which is not maintained and tested according to an entity's maintenance and testing program increases the likelihood that some of the UFLS equipment will not function as expected, URE not only has a variety of options to shed load automatically, but also has the option to manually shed load if circumstances warrant such an action. URE is staffed with NERC-certified operators and URE's SCADA system includes control and visibility of URE's power system. Failure of any single piece of UFLS equipment is unlikely to have a significant impact on the BPS and the likelihood of multiple pieces of equipment failing at the same time is low. Based on this, WECC determined this violation posed minimal risk to the BPS.

[26] *See supra* n. 15. As further background, 11 days before the Self-Report, WECC notified URE that an on-site compliance audit was scheduled. The notice letter served instructed URE to provide evidence of compliance with the NERC Reliability Standards applicable to URE as part of the upcoming audit, which included PRC-008-0 R2.

WECC201001850 PRC-011-0 R2

The purpose statement of PRC-011-0 provides: "Provide system preservation measures in an attempt to prevent system voltage collapse or voltage instability by implementing an Undervoltage Load Shedding (UVLS) program."

PRC-011-0 R2 provides: "The Transmission Owner and Distribution Provider that owns a UVLS system shall provide documentation of its UVLS equipment maintenance and testing program and the implementation of that UVLS equipment maintenance and testing program to its Regional Reliability Organization and NERC on request (within 30 calendar days)."

PRC-011-0 R2 has a "Lower" VRF and a "Severe" VSL.

URE self-reported a violation of PRC-011-0 R2. During an internal review, URE concluded that it had UVLS equipment that had not been maintained according to the intervals found in the URE Program. URE stated in its Self-Report that it did not document the maintenance and testing results for its batteries and PTs as required by PRC-011-0 R2. URE reported that 6 monthly inspections, 1 quarterly inspection, 2 annual inspections and 2 quarterly life capacity tests were incomplete, behind schedule, or missed on a number of its UVLS equipment batteries. The WECC SME determined that URE's PTs were being serviced within relay maintenance and testing intervals; however, the test results were not recorded with the relay maintenance and testing records unless the results were abnormal. As a result of URE's delinquent maintenance and testing on UVLS equipment batteries and its undocumented PT test results, URE could not demonstrate that its UVLS maintenance and testing program had been completely implemented. The SME did verify that the DC circuitry used for URE's UVLS program was being monitored at all times, which is an acceptable method for testing of this equipment. WECC determined that URE had a violation of PRC-011-0 R2 because it did not completely implement its UVLS equipment maintenance and testing program as required by the Standard.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because despite its failure to fully implement its maintenance and testing program, URE does monitor batteries and DC circuitry to evaluate their status and integrity. Furthermore, the failure of any single piece of UVLS equipment is unlikely to have a significant impact on the BPS. For these reasons, WECC determined this violation posed minimal risk to the BPS.

WECC201001823 TOP-002-2 R19

The purpose statement of TOP-002-2 provides: "Current operations plans and procedures are essential to being prepared for reliable operations, including response for unplanned events."

TOP-002-2 R19 provides: "Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations."

TOP-002-2 R19 has a "Medium" VRF and a "Severe" VSL.

URE reported a violation of TOP-002-2 R19 through both the Self-Report and Self-Certification process.[27] URE discovered during an internal compliance review that its operational planning computer models were inaccurate because they were based on inaccurate Facility Ratings. The Facility Ratings were not consistent with results based on URE's Facility Rating Methodology. URE confirmed to WECC SMEs that it found 26.5 % of its facilities had a different Facility Rating than the Facility Rating determined using its Facility Rating Methodology. WECC determined that URE had a violation of TOP-002-2 R19 because it failed to maintain accurate computer models for the analysis and planning of system operations

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS. Specifically, URE was utilizing Facility Ratings in its operations that were different than those produced using the URE Facility Rating Methodology. As a result, URE's computer models used for system forecasting provided inaccurate information. As a result of the incorrect models, there was a risk that URE's equipment would not function as forecasted in its computer models, potentially resulting in the misoperation of equipment, thereby posing moderate risk to the reliability to the BPS. This violation did not pose serious or substantial risk to the BPS because URE used industry standards and practices to rate its facilities and its system had performed successfully for many years with the ratings in place.

WECC201001826 TOP-005-1 R1

The purpose statement of TOP-005-1 provides: "To ensure reliability entities have the operating data needed to monitor system conditions within their areas."

TOP-005-1 R1 provides:

> Each Transmission Operator and Balancing Authority shall provide its Reliability Coordinator with the operating data that the Reliability Coordinator requires to perform operational reliability assessments and to coordinate reliable operations within the Reliability Coordinator Area.
>
> R1.1. Each Reliability Coordinator shall identify the data requirements from the list in Attachment 1-TOP-005-0 "Electric System Reliability Data"

[27] *See supra* n. 15.

> and any additional operating information requirements relating to operation of the bulk power system within the Reliability Coordinator Area.

TOP-005-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE reported a possible violation of TOP-005-1 R1 through both the Self-Report and Self-Certification process.[28] URE discovered during an internal compliance review that it failed to provide certain information requested by the Reliability Coordinator (RC), WECC. Specifically, URE stated in its Self-Report that on a specific date, the WECC RC requested that URE provide real-time indication via an Inter-Control Center Communications Protocol (ICCP) data link of URE's data for Automatic Voltage Regulators (AVRs) and the connection status of any generator over 50 MW within 73 days. URE operates two units at a specific generating site that are both rated over 50 MW, but URE failed to provide the required information for its first unit via ICCP data link until six months past the due date. URE did not report the information for its second unit via ICCP data link, which was later removed from service for a major overhaul. URE was providing the requested data to the WECC RC via a manual process instead of via ICCP. URE system dispatchers had a documented procedure to notify the WECC RC any time the first or second unit AVR was out of service and again when it was returned to service. WECC did have analog values for generator MW and breaker status, and the URE dispatcher sent the nightly spreadsheet with the 3-day forecast of expected load and available generation and operating reserves. The only data point not provided to the WECC RC was the generator kV.

In addition to the above incident, URE did not provide certain ICCP information requested by WECC in WECC's annual data request letter and spreadsheet. This was caused in part by URE personnel failing to recognize an additional data request that had been added from the previous year's request. The problem was also caused in part by WECC stating in the cover letter that accompanied the additional data request that all new data requests in the spreadsheet had been highlighted, when in fact WECC had only highlighted some but not all of the new data requests. WECC brought the matter to URE's attention when URE failed to provide the new data. URE immediately provided the requested data to WECC. WECC personnel subsequently acknowledged that URE had provided the data in time to allow WECC to update its model with no adverse consequences resulting from the late data submittal. WECC determined that URE had a violation of TOP-005-1 R1 because it failed to provide its RC with the operating data that the RC requires to perform operational reliability assessments and to coordinate reliable operations within the RC Area.

WECC determined the duration of the violation to be from when URE was late providing data related to its generating site, through when URE completed its first Mitigation Plan and from

[28] *See supra* n. 15.

when URE did not provide ICCP information as requested by WECC, through when URE provided the information six months later.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because while missing operational data potentially hampers the RC's ability to accurately model systems, URE provided the data in time to allow WECC to update its model with no adverse consequences resulting from the late data submittal. In addition, while the missing information represents a large percentage of generating capacity to the entity, it is a small amount in terms of the overall generation capacity of the BPS. For these reasons, WECC determined this violation posed minimal risk to the BPS.

WECC200902072 CIP-003-1 R5

The purpose statement of 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 R5 provides:

> Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>
> R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.
>
> R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
>
> R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
>
> R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

CIP-003-1 R5 has a "Lower" VRF and a "N/A" VSL.[29]

URE self-reported a violation of CIP-003-1 R5. Specifically, URE reported that it created a list of individuals to maintain a list of designated personnel responsible for authorizing logical or physical access. URE stated on the Self-Report that the list did not explicitly allow the individuals to authorize logical or physical access, but that the listed individuals understood that they had the authority to grant logical and physical access to protected information. URE further stated on the Self-Report that its list led to confusion when one of the listed individuals was replaced and the replacement individual did not realize that he had the authority to authorize logical or physical access to critical cyber asset information. URE had created an authorization list for approval/denial of unescorted physical access and cyber (electronic) access and identified the authorized individuals by name. The list identified individuals by name and title, however it did not include any phone numbers; nor did it state the information for which they were responsible for authorizing access. WECC determined that URE had a violation of CIP-003-1 R5 because it failed to create a list of designated personnel who are responsible for authorizing logical or physical access to protected information that included business phone numbers and the information for which they are responsible for authorizing access.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because prior to when the Standard became enforceable, URE established and implemented procedures and practices to protect its CCA information. Under its procedures, URE granted CCA protected information access only to those requesting individuals who had a legitimate business need for the information, an acceptable personal risk assessment and CIP training. For these reasons, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC200902070 CIP-004-1 R4

The purpose statement of 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."

[29] *See supra* n. 17.

CIP-004-1 R4 provides:

> 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 "Medium" VRF and a "N/A" VSL.[30]

URE self-reported a violation of CIP-004-1 R4. Specifically, URE self-reported that it failed to revoke access for an employee that moved to a new position within seven calendar days of the employee no longer requiring authorized cyber or authorized unescorted physical access to CCAs. A URE employee with physical access to CCAs transferred to a new position. The employee's new position within URE did not require the individual to have access to CCAs. Seven days later, the employee's supervisor initiated a process to revoke the employee's access to CCAs. Two days after that, the employee's supervisor approved the revocation of the employee's physical access to CCAs. URE's facility's operation manager revoked the employee's access to CCAs; 14 days after the employee no longer required access. WECC determined that URE had a violation of CIP-004-1 R4 because URE failed to revoke access for an employee within seven calendar days of the employee no longer requiring such access to CCAs.

WECC determined the duration of the violation to be from seven days after the employee no longer required access to CCAs, through when URE revoked the employee's access.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because the individual with unauthorized access to the CCAs was an employee that had previously been authorized and simply changed positions within URE. In addition, the

[30] *See supra* n. 17.

employee's access was revoked 14 days after the employee no longer required access. For these reasons, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC201002084 CIP-005-1 R2

The purpose statement of 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 provides:

> 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).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
>
> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
>
> R2.5. The required documentation shall, at least, identify and describe:
>
> R2.5.1. The processes for access request and authorization.
>
> R2.5.2. The authentication methods.
>
> R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

> R2.5.4. The controls used to secure dial-up accessible connections.
>
> R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R2 has a "Medium" VRF and a "N/A" VSL.[31]

URE submitted a Self-Certification indicating it had a violation of CIP-005-1 R2.2. During an internal review, URE discovered a number of devices that were not reviewed to determine enabled ports and services. As a result, these devices had ports and services enabled that were not required for operations and for monitoring Cyber Assets within its Electronic Security Perimeter (ESP). Furthermore, URE did not document the configuration of the ports and services for these devices. WECC determined that URE had a violation of CIP-005-1 R2 because URE failed to enable only ports and services required for operations and for monitoring Cyber Assets on the identified devices; URE also failed to document the configuration of those ports and services for the same devices.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS. Specifically, failure to ensure that only those ports and services required for operations and monitoring Cyber Assets within the ESP are enabled poses risk to the entity's Cyber Assets. This increased risk may allow for unauthorized internal or external access, which could allow for successful cyber attacks against CCAs. In this case, URE failed to enable only those ports and services required for operations and for monitoring Cyber Assets within the ESP. This violation did not pose a severe risk to the BPS because the violation is limited to the identified devices and URE has monitoring and logging of system events in place.

WECC201002119 CIP-006-2 R1

The purpose statement of CIP-006-2 provides in pertinent part: "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."

[31] *See supra* n. 17.

CIP-006-2 R1 provides:

> Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
> >
> > R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
> >
> > R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.
> >
> > R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.
> >
> > R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
> >
> > R1.8. Annual review of the physical security plan.

CIP-006-2 R1 has a "Medium" VRF and a "Severe" VSL.[32]

[32] On December 18, 2009, NERC submitted revised VRFs and VSLs for CIP-002-2 through CIP-009-2. On January 20, 2011, FERC issued an order approving the Version 2 VRFs and VSLs and made them effective on April 1, 2010, the date the Version 2 CIP Reliability Standards became effective.

URE self-reported a violation of CIP-006-2 R1. Specifically, URE reported that it discovered an incident where an unauthorized employee was left unescorted within URE's Physical Security Perimeter (PSP). On a single day, an employee without authorized unescorted access rights was escorted by an authorized individual to a conference room located within URE's PSP in accordance with URE's procedures. After entering the conference room, the escort left the conference room, leaving the unauthorized employee unattended within the PSP. Later, URE personnel escorted several other unauthorized employees to the conference room to participate in a meeting. During the course of the meeting, one or more of the unauthorized employees intermittently stepped out of the conference room unescorted to use mobile telephones. WECC determined that URE had a violation of CIP-006-2 R1 because URE did not provide continuous escorted access for unauthorized personnel within URE's PSP.

WECC determined the duration of the violation to be one day, when the unauthorized personnel were not continuously escorted.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because there was only one CCA within a very large PSP at this location. Furthermore, URE determined that the individual left unescorted in the conference room was an employee that never left the room, and the individuals who stepped outside to use mobile phones never approached the CCA. For these reasons, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC201002089 CIP-006-1 R2

CIP-006-1 R2 provides:

> Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> > R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

> R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" VRF and a "N/A" VSL.[33]

URE self-reported a possible violation of CIP-006-1 R2. Specifically, URE reported that a retiring employee's CCA physical access was erroneously reinstated. An employee was scheduled to retire, and, pursuant to URE's physical access procedural controls, URE would revoke the employee's physical access rights effective the employee's final day of scheduled work. However, due to an internal error one week prior to that final day of scheduled work, some URE access cards failed to work correctly. To correct this issue, URE's physical security vendor changed the access privileges for all personnel to expire at the same date and time (specifically, a date ten days past the identified employee's scheduled retirement date). As a result, the retiring employee's access rights were changed to that date, beyond the known retirement date. URE conducted a quarterly review of its access control matrix and determined that the retired employee had retained access privileges 10 days beyond the last date the employee had authorized access to enter the PSP. WECC determined that URE had a violation of CIP-006-1 R2 because URE failed to implement the operational and procedural controls to manage physical access at all access points to its PSP twenty-four hours a day, seven days a week.

WECC determined the duration of the violation to be from when URE should have revoked access for the retiring employee, through the date URE revoked access for the retiring employee and demonstrated to a WECC SME the individual's current access right was listed as "inactive."

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE had a current PRA on file for the retiring employee and the individual in question had completed cyber security training prior to retirement. Furthermore, URE confirmed that the individual did not enter the PSP for more than 3 weeks before the effective retirement date because the person in question effectively began retirement by using unused vacation time. Further, URE had documented operational and procedural control in place at the time of the violation. Lastly, the employee involved was a long-time URE employee. For these reasons WECC determined this violation posed a minimal risk to the reliability of the BPS.

<u>WECC201002113 CIP-006-2 R2</u>
CIP-006-2 R2 provides:

> Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at

[33] *See supra* n. 17.

the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

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

CIP-006-2 R2 has a "Medium" VRF and a "Severe" VSL.[34]

URE self-reported a violation of CIP-006-2 R2. Specifically, URE reported that a URE communication technician inadvertently provided an unauthorized access point through the access control system's (ACS) ESP. A customer service manager was originally given the ability to view security cameras (CCTV) located in the customer service lobby on a monitor located in his office as part of a remodeling project. The connection path to the video was delivered through a client computer located in the customer service manager office to a network cable, then through a Virtual LAN (VLAN) connection to the camera's digital video recorder (DVR). Originally, when URE implemented its compliance plan for CIP, URE established an ESP around the access control network and the CCTV feed from the DVRs to the customer service manager's client computer was disabled. At that time, the customer service manager requested that URE find a solution to allow the customer service manager to view the cameras. Forty-two days prior to the Self-Report, a technician reconnected the CCTV client computer in the customer service manager's office and added it to the existing access control system's client VLAN. The new access was connected through the ESP and ACS firewall so the client computer could have login and password authentication through the ACS. The result of the change was that the technician had inadvertently provided an unauthorized access point through the ACS's ESP. WECC determined that URE had a violation of CIP-006-2 R2 because URE failed to implement URE's processes for access request and authorization for control of electronic access at all electronic access points to the ESP.

WECC determined the duration of the violation to be from when the unauthorized access point was connected, through when URE disconnected the connection through the ACS's ESP ten days later.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE discovered and corrected the error just ten days after the risk was created and the unauthorized access point was physically located on the URE premises and

[34] *See supra* n. 32.

accessible only by URE employees. For these reasons, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC201002060 CIP-007-1 R2

The purpose statement of 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 R2 provides:

> 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.
>
> R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "N/A" VSL.[35]

URE submitted a Self-Certification indicating a violation of CIP-007-1 R2. URE did not have a documented procedure in place to ensure only ports and services required for normal and emergency operations were enabled. As a result, the URE had discovered multiple open ports that were not required to be open for normal or emergency operation. Furthermore, URE had recently discovered additional ports and services since the time of Self-Certification that were still open. URE personnel identified two additional issues not discovered at the time of Self-Certification. URE discovered the first issue during a vulnerability assessment. The assessment found that URE has EMS client workstations with open ports that were not required for normal or emergency operations. Following the vulnerability assessment, URE closed all non-essential ports and services on the EMS client workstations. URE staff discovered a server that had a

[35] *See supra* n. 17.

protocol turned on which URE used for logging and management purposes; however, it no longer used it as an essential service for the server and thus was not required for normal or emergency operation. URE did not have a process in place to identify these types of open ports, thus URE did not identify these ports when initially self-certifying. WECC determined that URE had a violation of CIP-007-1 R2 because URE failed to establish and document a process to ensure that only ports and services required for normal and emergency operations are enabled.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS. Specifically, in this instance, there was a lack of awareness regarding URE's ports and services. Also, URE failed to have a documented procedure for ensuring that only required ports and services are enabled. Without knowledge of which ports and services are open and available, unauthorized access to Cyber Assets and or CCAs may be obtained through an open port. This increases the likelihood of a loss of control and potential misuse of critical assets and systems. This violation did not pose a serious or substantial risk to the BPS due the number of devices involved and the testing of URE's active and passive security controls. URE discovered this violation upon conducting a vulnerability assessment because URE does monitor and log system events.

WECC201002067 CIP-007-1 R3
CIP-007-1 R3 provides:

> 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, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "N/A" VSL.[36]

URE submitted a Self-Certification indicating a violation of CIP-007-1 R3. A URE internal audit discovered that URE failed to document applicable cyber security software patches for all Cyber Assets within the ESP(s).[37] Specifically, URE failed to conduct and document an assessment of security patches and security upgrades for its EMS servers and workstations, as well as supporting network equipment. URE also failed to document the implementation of applicable security patches or upgrades or document compensating measures that shall be applied to mitigate risk exposure or an acceptance of risk when patches were not installed. URE's audit determined that a number of devices were not patched or upgraded as required by the Standard. WECC determined that URE had a violation of CIP-007-1 R3 because URE failed to document the assessment of security patches and security upgrades for applicability; failed to document the implementation of applicable security patches or upgrades; and failed to document compensating measures that shall be applied to mitigate risk exposure or an acceptance of risk, when patches were not installed for the identified Cyber Assets within URE's ESP.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because the identified devices involved in this incident are not connected to the internet, meaning system risk and exposure is greatly reduced. For this reason, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC201002061 CIP-007-1 R5

CIP-007-1 R5 provides:

> 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.

[36] *See supra* n. 17.

[37] The violation of CIP-007-1 R3 is specific to URE's Energy Management System (EMS) servers and workstations, as well as supporting network equipment.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 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.

R5.2.3. 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).

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

R5.3.1. Each password shall be a minimum of six characters.

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

> R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-1 R5 has a "Lower" VRF and a "N/A" VSL.[38]

URE submitted a Self-Certification indicating a violation of CIP-007-1 R5. URE failed to establish methods, processes and procedures that would allow for the generation of logs for some of its user account access activity. Specifically, URE had established and implemented procedural controls for user access that minimized the risk of unauthorized system access; however, its initial version of the URE account management procedure did not set forth a method, process or procedure to allow adequate logging for its individual or shared user accounts access activity. WECC determined that URE had a violation of CIP-007-1 R5 because URE failed to establish methods, processes and procedures that would result in the generation of logs of sufficient detail to create historical audit trails of individual user account access activity.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE had implemented access controls that addressed the fundamental issues of user access controls. For this reason, WECC determined this violation posed minimal risk to the reliability of the BPS.

WECC201002066 CIP-007-1 R6
CIP-007-1 R6 provides:

> Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

[38] *See supra* n. 17.

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

CIP-007-1 R6 has a "Medium" VRF and a "N/A" VSL.[39]

URE submitted a Self-Certification indicating a violation of CIP-007-1 R6. During a quarterly compliance review, URE identified that it had no security logging available for a number of Cyber Assets within its ESP. URE contracted with a vendor to help it implement software that allows users to conduct logging and security status and monitoring across an EMS network. In the course of the software implementation, a number of network devices were overlooked. URE proceeded with its roll out of the software. Subsequently, during a quarterly review, the entity identified that 15% of its network devices were not producing logs, as required by this Standard. URE conducted an internal investigation and discovered that the identified devices were not configured to allow the software to pull a log file. WECC determined that URE had a violation of CIP-007-1 R6 because URE failed to implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, URE failed for 15% of its Cyber Assets to establish monitoring controls that issue automated or manual alerts for detected Cyber Security Incidents as required by R.6.2; failed to maintain logs of system events related to cyber security as required by R6.3; and failed to retain logs for ninety calendar days as required by R6.4.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE had implemented access controls that addressed the fundamental issues of user access controls. For this reason, WECC determined this violation posed minimal risk to the reliability of the BPS.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred thirty-five thousand dollars ($135,000) for the referenced violations. In reaching this determination, WECC considered the following factors: (1) VRF; (2) VSL; (3) risk to the reliability of the BPS,

[39] *See supra* n. 17.

including the seriousness of the violation; (4) violation time horizon; (5) the violation's duration; (6) the Registered Entity's negative compliance history; (7) the Registered Entity's Self-Reports of PRC-011-0 R2, CIP-003-1 R5, CIP-004-1 R4, CIP-006-2 R1, CIP-006-1 R2 and CIP-006-2 R2 and voluntary corrective action; (8) the degree and quality of cooperation by the Registered Entity in the audit or investigation process, and in any remedial action; (9) the quality of the Registered Entity's compliance program; (10) any attempt by the Registered Entity to conceal the violation or any related information; (11) whether the violation was intentional; (12) any other relevant information or extenuating circumstances; and (13) the Registered Entity's ability to pay a penalty, as applicable.

URE supplied an explanatory statement which is incorporated into the Settlement Agreement with respect to the instant violations of PRC-005-1 R2, PRC-008-0 R2 and PRC-011-0 R2. That statement is as follows:

> There are varying interpretative approaches to developing and implementing the maintenance and testing program required by PRC-005, PRC-008 and PRC-011. [URE] developed a very stringent maintenance and testing program that is a robust superset of the industry's most aggressive best practices. The program's scheduled testing intervals were very stringent to ensure that any gaps in testing timelines would have no impact on the reliability of [URE]'s Protection System. In other words, [URE] set the maintenance and testing intervals so tightly that there would be little or no risk to the reliability of the system if a testing or maintenance deadline were missed. However, in doing so, [URE] left itself little or no room for scheduling flexibility. [URE] has since broadened its maintenance testing intervals, which are still well within accepted industry best practices, to ensure it meets maintenance and testing intervals for reporting purposes.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred thirty-five thousand dollars ($135,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[40]

WECC201001853 BAL-005-0 R17
URE's Mitigation Plan to address its violation of BAL-005-0 R17 was submitted to WECC on February 24, 2010 with a proposed completion date of April 30, 2010. The Mitigation Plan was accepted by WECC on March 12, 2010 and approved by NERC on March 25, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2010 in accordance with FERC orders.

[40] *See* 18 C.F.R § 39.7(d)(7).

URE's Mitigation Plan required URE to:

1. Develop and implement a procedure to annually check and document the accuracy of all frequency transducers;
2. Establish an annual maintenance tracking program;
3. Check and document the accuracy of all frequency transducers utilized for AGC; and
4. Replace any frequency transducers that do not meet the accuracy standards for analog and digital frequency transducers as applicable.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted several Excel files and certificate of calibration notification sheets.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001880 CIP-002-1 R1

URE's Mitigation Plan to address its violation of CIP-002-1 R1 was submitted as complete to WECC on April 11, 2011. The Mitigation Plan was accepted by WECC on June 15, 2011 and approved by NERC on July 20, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on July 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan stated that URE had revised its RBAM to incorporate NERC recommendations and guidance after receiving the NERC Security Guideline in September 2009.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its Critical Asset identification process and RBAM procedure to the CIP Spot Check team at the time of the Spot Check.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001881 CIP-002-1 R3

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC on July 6, 2010 stating that it had been completed on June 30, 2009. The Mitigation Plan was accepted by WECC on September 2, 2010 and approved by NERC on October 5, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 6, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to develop a list of individual components associated with its CCAs, to be reviewed at least annually.

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

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001819 FAC-009-1 R1

URE's Mitigation Plan to address its violation of FAC-009-1 R1 was submitted to WECC on February 11, 2010 stating it had been completed February 9, 2010. The Mitigation Plan was accepted by WECC on February 19, 2010 and approved by NERC on March 3, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 3, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise URE's Facility Ratings Methodology;
2. Compare all URE Facility Ratings against the revised methodology and determine the correct rating of all URE BPS facilities based on the most limiting factor;
3. Notify all stakeholders of revised Facility Ratings; and
4. Develop and implement a procedure for assuring all Facility Ratings are updated and reported as changes to facility components occur.

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

1. A Facility Rating line document and several reduction letters;
2. Response to Facility Ratings Methodology changes procedure;
3. Facility Ratings Methodology procedure; and
4. Facility Ratings for individual pieces of equipment.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001824 PER-001-0 R1

URE's Mitigation Plan to address its violation of PER-001-0 R1 was submitted to WECC on February 6, 2010 stating it had been completed on January 18, 2010. The Mitigation Plan was accepted by WECC on February 12, 2010 and approved by NERC on March 3, 2010. The

Mitigation Plan for this violation was submitted as non-public information to FERC on March 3, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise the real time energy trader job description to clearly outline the responsibilities and authorities of URE's real time energy traders;
2. Revise the job description to clearly state that real time energy trader personnel are responsible for complying with the NERC Reliability Standards;
3. Revise the job description to clearly state that during normal and emergency conditions, real time energy traders have the authority to take or direct timely and appropriate real-time actions and those such actions can be performed without obtaining approval from higher-level management; and
4. Make the revised job description readily accessible in the control room environment to all operating personnel.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its real time energy trader job description, and states that a real time energy trader is responsible for complying with NERC Standards. The policy also makes clear that real time energy traders have the authority to take direct timely and appropriate real-time actions, and such actions can be taken without approval from higher-level management during normal and emergency conditions, which outlined the responsibilities and authorities of the position.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001848 PRC-005-1 R2

URE's Mitigation Plan to address its violation of PRC-005-1 R2 was submitted to WECC on March 3, 2010 with a proposed completion date of February 25, 2011. The Mitigation Plan was accepted by WECC on March 17, 2010 and approved by NERC on March 25, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Maintain and test URE's relays, communications equipment, voltage and current sensing devices, batteries and DC circuitry according to the URE Program;
2. Develop a tracking procedure, including testing intervals into maintenance tracking software; and
3. Complete past due maintenance and testing.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a PRC-005-1 R2 mitigation completion summary memorandum that included maintenance and testing data.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001849 PRC-008-0 R2

URE's Mitigation Plan to address its violation of PRC-008-0 R2 was submitted to WECC on March 3, 2010 with a proposed completion date of May 28, 2010. The Mitigation Plan was accepted by WECC on March 11, 2010 and approved by NERC on March 25, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop tracking procedures for the voltage and current sensing devices, batteries and DC circuitry used in URE's UFLS maintenance and testing program;
2. Include testing intervals into maintenance tracking software; and
3. Complete past due maintenance and testing.

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

1. Training material and attendance reports;
2. Flow charts for relays, station batteries and PT devices;
3. Screen shots of the maintenance tracking systems; and
4. Protection System maintenance and testing tracking documents.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001850 PRC-011-0 R2

URE's Mitigation Plan to address its violation of PRC-011-0 R2 was submitted to WECC on March 3, 2010 with a proposed completion date of May 28, 2010. The Mitigation Plan was accepted by WECC on March 7, 2010 and approved by NERC on March 25, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 25, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Set up equipment specific maintenance management tracking functions and notifications in its enterprise resource planning software;
2. Perform infrared inspections of all standing and external PTs consistent with the current Protection System maintenance and testing program; and
3. Strengthen its maintenance and testing program for DC circuitry to include more detailed procedures, interval definitions and documentation requirements.

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

1. Training material and attendance reports;
2. Flow charts for relays, station batteries, PT devices and CT circuitry;
3. Screen shots of maintenance tracking systems; and
4. Protection System maintenance and testing tracking documents.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001823 TOP-002-2 R19

URE's Mitigation Plan to address its violation of TOP-002-2 R19 was submitted to WECC on February 18, 2010 stating a completion date of February 9, 2010. The Mitigation Plan was accepted by WECC on February 20, 2010 and approved by NERC on March 10, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 10, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review and verify the URE Facility Ratings Methodology and revise as necessary;
2. Compare all URE Facility Ratings against the re-verified methodology and determine the correct rating of all URE BPS facilities based on the most limiting factor;
3. Notify all stakeholders of the revised Facility Rating; and
4. Develop and implement a procedure for assuring all Facility Ratings are updated and reported as changes occur to facility components.

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

1. Response to Facility Ratings Methodology changes procedure; and

2. Documented communications between URE employees concerning the updated Facility Ratings.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201001826 TOP-005-1 R1

URE's Mitigation Plan to address its violation of TOP-005-1 R1 was submitted to WECC on February 25, 2010 stating it had been completed on February 17, 2010. The Mitigation Plan was accepted by WECC on February 26, 2010 and approved by NERC on March 12, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 12, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Evaluate and define the formulas necessary for the calculation of the user console status in the EMS;
2. Confirm data integration plan with WECC RC;
3. Transmit available data to WECC RC via ICCP link: first unit AVR, first unit user console, second unit user console; and
4. Take the second unit off-line for rebuilding.

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

1. Letter regarding the status of data request completion from the WECC RC; and
2. Email regarding the second unit's scheduled outage.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC200902072 CIP-003-1 R5

URE's Mitigation Plan to address its violation of CIP-003-1 R5 was submitted to WECC on November 30, 2009 stating it had been completed November 25, 2009. The Mitigation Plan was accepted by WECC on September 10, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 7, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its program for managing access to protected CCA information and to eliminate confusion by modifying its list of designated personnel who can grant access to CCA

information by ensuring that the list now contains names, titles, phone numbers and the protected CCA information for which they are responsible for authorizing access; and

2. Inform personnel of the changes, revise its training on the CCA information protection procedure and conduct training on the new procedure.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted its revised CCA information protection procedure.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC200902070 CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to WECC on December 23, 2009 stating it had been completed on November 7, 2009. The Mitigation Plan was accepted by WECC on September 7, 2010 and approved by NERC on October 5, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 6, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revoke access for the identified employee moved to a position not requiring CCA access;
2. Revise the control procedure for Cyber and unescorted physical access to CCAs and its associated form to clarify and simplify the process for revoking access to CCAs to ensure the process is easily understood;
3. Advise the managers, supervisors and staff who are responsible for the process of the changes;
4. Create a document which summarizes the CCA access revocation process's work flow for revoking access;
5. Provide this document to those managers, supervisors and staff responsible for the access revocation process; and
6. Review the document with them and answer questions.

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

1. Application for CCA access revocation document;
2. Cardholder tracking report document; and
3. CCA access control matrix of employees removed document.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002084 CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC on March 4, 2010 with a proposed completion date of May 30, 2010. The Mitigation Plan was accepted by WECC on September 14, 2010 and approved by NERC on October 7, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 7, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Evaluate all four access points to the EMS ESP;
2. Further analyze the following items associated with two access points due to lack of vendor information;
    a. WECC email communications: Using information provided by WECC technical personnel, URE has enabled only the required ports from the designated WECC email servers to the URE's email client. This work was performed at the cutover to new WECC email servers and eliminates previous servers.
    b. WECC anti-virus communications: Using information provided by WECC technical personnel, URE disabled communications ports between its WECC email client and the WECC anti-virus servers which are no longer required. URE's WECC email client exists within an ESP and utilizes the anti-malware products used by the other Cyber Assets within this ESP.
    c. Communications for management: Steps have been taken to enable only operational communications for part of URE's management section data queries to the server.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted mitigation evidence files including the configuration to tighten down ports used in the communications for management and a change request.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002119 CIP-006-2 R1

URE's Mitigation Plan to address its violation of CIP-006-2 R1 was submitted to WECC on September 11, 2010 stating it had been completed as of August 27, 2010. The Mitigation Plan was accepted by WECC on September 22, 2010 and approved by NERC on October 8, 2010. The

Mitigation Plan for this violation was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

URE's Mitigation Plan required:

1. The responsible manager to give refresher training to escorts;
2. An article reviewing escort requirements and procedures within PSPs was placed in the monthly security awareness newsletter that is emailed to employees; and
3. URE updated CIP-006 R4 procedure with additional guidance for escorts.

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

1. A file that provided a narrative summary and supporting evidence for the Mitigation Plan;
2. A redline physical access controls procedure document;
3. The physical access controls procedure document; and
4. Two internal emails.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002089 CIP-006-1 R2

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC on April 19, 2010 stating it had been completed on April 15, 2010. The Mitigation Plan was accepted by WECC on June 10, 2011 and approved by NERC on July 20, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on July 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revoke access to the identified employee;
2. Revise its physical access control procedure to include a new statement regarding which tasks should be completed by facilities maintenance; and
3. Communicate the updated procedure to the appropriate managers/supervisors who supervise employees who work on the ACS.

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

1. Physical access control procedure; and

2. A copy of the email to access control supervisors.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002113 CIP-006-2 R2

URE's Mitigation Plan to address its violation of CIP-006-2 R2 was submitted to WECC on September 11, 2010 stating it had been completed on August 27, 2010. The Mitigation Plan was accepted by WECC on September 21, 2010 and approved by NERC on October 8, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Disconnect the unauthorized access point connection through the ACS's ESP;
2. Have the supervisor meet with the technicians who have administrative rights to modify access to the ACS ESP, review the CIP-004-2 R4 procedure and discuss the importance of understanding and following the procedure; and
3. Improve and implement the procedural documentation in URE's CIP-004-2 R4 procedure in order to clarify the process for granting access through an 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 access revocation report;
2. CIP-004-2 R4 procedure; and
3. A mitigation narrative.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002060 CIP-007-1 R2

URE's Revised Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC on September 3, 2010 with a proposed completion date of September 17, 2010. The Mitigation Plan was accepted by WECC on September 22, 2010 and approved by NERC on October 8, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review existing documentation of ports and services in two reference documents;

2. Compare the known ports and services lists to data collected in a recent CIP-007 R1 test event. CIP-007 R1 testing requires collection of ports and services in use on systems within the development environment.
3. Conduct ports and services audits on the EMS systems and combine the data into a single spreadsheet for analysis;
4. Conduct a risk assessment using the ports and services combined data report per the CIP-007 R2 procedure;
5. Test the proposed disable list; and
6. Deploy configuration changes in production.

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

1. Ports and services combined data report;
2. Deploy configuration changes in production deployment plan; and
3. The CIP-007 R2 procedure.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002067 CIP-007-1 R3

URE's Revised Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC on June 17, 2010 with a proposed completion date of July 30, 2010.[41] The Mitigation Plan was accepted by WECC on September 1, 2010 and approved by NERC on November 19, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on November 22, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Assign additional staff to assess and document applicable security patches;
2. Commence performing and documenting a risk assessment of applicable security patches;
3. Implement automated tools to assist in patch identification;

[41] On October 6, 2010, NERC submitted an approved Mitigation Plan for NERC Violation Tracking ID# WECC201002067 for URE. WECC subsequently submitted this revised Mitigation Plan to NERC in which URE added steps to resolve the security patch application issue. The target completion changed from June 28, 2010 to July 30, 2010

4. Implement a system to proactively check for new vulnerabilities published in the National Vulnerability Database; and
5. Commence update and revision of the security patch management procedures.

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

1. Memorandum narrative summary of mitigation completion;
2. Patch management spreadsheet;
3. Patch management event test procedure checklist;
4. Patch management procedure*;*
5. CIP-007 R3 flowchart of narrative process steps; and
6. Patch management tracking form.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violation of the Standard.

WECC201002061 CIP-007-1 R5
WECC201002066 CIP-007-1 R6

URE's Mitigation Plan to address its violations of CIP-007-1 R5 and R6 was submitted to WECC on September 3, 2010 stating it had been completed on August 27, 2010. The Mitigation Plan was accepted by WECC on September 22, 2010 and approved by NERC on October 8, 2010. The Mitigation Plan for these violations was submitted as non-public information to FERC on October 8, 2010 in accordance with FERC orders.

URE's Mitigation Plan stated URE had:

1. Revise its account management procedure to clarify the method, process and procedures needed to generate an audit trail of logs for activities related to individual and shared use accounts;
2. Create a new format of the CIP-007 R5 account management procedure to better track and manage all accounts;
3. Disable all unnecessary shared accounts, document the necessary shared accounts, rename identified administrative accounts, implement a new logon/logoff policy and take steps to ensure that password changes are enforced on all systems for all accounts;
4. Complete final revisions to its CIP-007 R5 account management procedure and appendices to include a method, process and procedure to effectively manage all EMS and ACS accounts;

5. Send an email to authorized individuals to inform them that the procedure had been updated and revised; and
6. Confirm and document that the remaining EMS devices have been configured to generate security event logging.

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

1. WECC data request narrative;
2. CIP-007 R5 account management procedure;
3. Redlined CIP-007 R5 account management procedure; and
4. Several evidence documents.

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed and that URE had mitigated the violations of the Standard.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[42]

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,[43] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 12, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred thirty-five thousand dollar ($135,000) 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. WECC considered URE's violation history;
2. URE self-reported the PRC-011-0 R2, CIP-003-1 R5, CIP-004-1 R4, CIP-006-2 R1, CIP-006-1 R2 and CIP-006-2 R2 violations;

[42] *See* 18 C.F.R. § 39.7(d)(4).

[43] *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).

3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program which WECC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC 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 thirty-five thousand dollars ($135,000) 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 parts of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between WECC and URE executed August 25, 2011, included as Attachment a;

b) Record documents for WECC201001853 BAL-005-0 R17, included as Attachment b:

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

c) Record documents for WECC201001880 CIP-002-1 R1, included as Attachment c:

   1. URE's Source Document for WECC201001880 CIP-002-1 R1 and WECC201001881 CIP-002-1 R3;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion;

4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for WECC201001881 CIP-002-1 R3, included as Attachment d:

1. URE's Mitigation Plan;
2. URE's Certification of Mitigation Plan Completion;
3. WECC's Verification of Mitigation Plan Completion;

e) Record documents for WECC201001819 FAC-009-1 R1, included as Attachment e:

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

f) Record documents for WECC201001824 PER-001-0 R1, included as Attachment f:

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

g) Record documents for WECC201001848 PRC-005-1 R2, included as Attachment g:

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

h) Record documents for WECC201001849 PRC-008-0 R2, included as Attachment h:

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

i) Record documents for WECC201001850 PRC-011-0 R2, included as Attachment i:

1. URE's Source Document;

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

j) Record documents for WECC201001823 TOP-002-2 R19, included as Attachment j:

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

k) Record documents for WECC201001826 TOP-005-1 R1, included as Attachment k:

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

l) Record documents for WECC200902072 CIP-003-1 R5, included as Attachment l:

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

m) Record documents for WECC200902070 CIP-004-1 R4, included as Attachment m:

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

n) Record documents for WECC201002084 CIP-005-1 R2, included as Attachment n:

1. URE's Source Document;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;

4. WECC's Verification of Mitigation Plan Completion;

o) Record documents for WECC201002119 CIP-006-2 R1, included as Attachment o:

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

p) Record documents for WECC201002089 CIP-006-1 R2, included as Attachment p:

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

q) Record documents for WECC201002113 CIP-006-2 R2, included as Attachment q:

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

r) Record documents for WECC201002060 CIP-007-1 R2, included as Attachment r:

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

s) Record documents for WECC201002067 CIP-007-1 R3, included as Attachment s:

1. URE's Source Document;
2. URE's Revised Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

t) Record documents for WECC201002061 CIP-007-1 R5 and WECC201002066 CIP-007-1 R6, included as Attachment t:

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

A Form of Notice Suitable for Publication[44]

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

[44] *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 Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz	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 Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz *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 30326-1001
(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
Western Electricity Coordinating Council

Attachments