July 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 1, Unidentified Registered Entity 2, Unidentified Registered Entity 3, and Unidentified Registered Entity 4 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 1 (URE1), Registry ID# NCRXXXXX, Unidentified Registered Entity 2 (URE2), Registry ID# NCRXXXXX, Unidentified Registered Entity 3 (URE3), Registry ID# NCRXXXXX, and Unidentified Registered Entity 4 (URE4), NERC Registry ID# NCRXXXXX, (collectively UREs), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

URE1 self-reported a violation[3] of CIP-004-1[4] Requirement (R) 3 to Western Electricity Coordinating Council (WECC) for URE1's failure to perform a personnel risk assessment (PRA) for one employee

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

[2] *See* 18 C.F.R § 39.7(c) (2).

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

[4] At the time of UREs' violations, Version 1 of the CIP Standards was in effect and was mandatory and enforceable for these entities. CIP Version 1 became effective on July 1, 2008 and remained enforceable through March 31, 2010. CIP Version 2 was approved by the Commission and became enforceable on April 1, 2010 and was enforceable through September 30, 2010. CIP Version 3 was approved by the Commission and became enforceable on October 1, 2010 and remained

within 30 days of that employee being granted access to a URE1 control center. URE1 self-reported violations of CIP-006-1 R2, R3 and R4 to WECC. URE1 failed to implement the required procedural and operational controls to manage physical access at all access points to its Physical Security Perimeter (PSP) when URE1 allowed unauthorized personnel physical access when one of its janitors used a "hard key" to open a door gaining access to a Critical Cyber Asset (CCA) in violation of CIP-006-1 R2. URE1 failed to implement appropriate responses to access control alarms in violation of CIP-006-1 R3. Finally, URE1 failed to document individuals who had access to CCAs on multiple occasions, in violation of CIP-006-1 R4.

URE2 self-certified[5] a violation of CIP-006-1 R2[6] to WECC for URE2's failure to implement the procedural and operational controls to manage physical access at all access points to a PSP and failure to properly configure card access to a PSP which allowed unauthorized personnel physical access to points on URE2's PSP.

URE3 self-reported a violation of PRC-005-1 R1.1 to WECC for URE3's failure to define maintenance and testing intervals for newly-installed Protection System[7] equipment.

URE4 self-certified a violation of CIP-003-1 R4 to WECC, and URE4 followed-up its self-certification with a Self-Report for violations of CIP-003-1 R4.2 and R5.1. URE4 was in violation of CIP-003-1 R4.2 because URE4's program for managing protected information associated with CCAs lacked a process for identifying and releasing protected information to third-party vendors. URE4 was in violation of CIP-003-1 R5.1 because it did not identify the name and title of a construction manager who released CIP information to outside vendors, as well as not identifying the information for which the construction manager was responsible. URE4 self-certified a violation of CIP-004-1 R2 and R3 to WECC and, URE4 followed-up its Self-Certification with a Self-Report for violations of CIP-004-1 R2 and R4. URE4 was in violation of CIP-004-1 R2 by failing to train a number of employees with access to CCAs within 90 days of their being granted such access. URE4 was in violation of CIP-004-1 R4 because URE4

---

enforceable through the end duration date of the CIP violations included in this filing. For consistency in this filing, Version 1 of the CIP Standards is used throughout.

[5] The Settlement Agreement states the discovery method as "Self-Report." URE2 self-reported this violation during its self-certification period, and, because at the time of the Self-Report, URE2 had an existing obligation to self-certify to WECC whether it was compliant, it did not receive Self-Report credit in this case.

[6] URE2 originally self-certified a violation of CIP-004-1 R4 but after reviewing the record, WECC's Compliance Enforcement Department concluded that the appropriate Standard in this case was CIP-006-1 R2 and not CIP-004-1 R4.

[7] *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."

did not remove certain employees from its list of personnel with access to CCAs after those employees were no longer permitted access to the CCAs within the time period required by the Standard.

This Notice of Penalty is being filed with the Commission because WECC and UREs have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-004-1 R3 and CIP-006-1 R2, R3 and R4 for URE1, CIP-006-1 R2 for URE2, PRC-005-1 R1.1 for URE3, and CIP-003-1 R4.2 and R5.1, and CIP-004-1 R2 and R4 for URE4. According to the Settlement Agreement, UREs agrees and stipulates to the facts of the violations and has agreed to the assessed penalty of one hundred thirty-four thousand three hundred fifty dollars ($134,350), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201002298, WECC201002406, WECC201002299, WECC201002300, WECC201002379, WECC201002257, WECC201002253, WECC201002254, WECC201002258 and WECC201002259 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 May 30, 2012, by and between WECC and UREs, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity 1	NOC-1123	WECC201002298	CIP-004-1	3	Medium[8]	$134,350
			WECC201002406	CIP-006-1	2	Medium	
			WECC201002299	CIP-006-1	3	Medium	
			WECC201002300	CIP-006-1	4	Lower	
	Unidentified Registered Entity 2		WECC201002379	CIP-006-1[9]	2	Medium	
	Unidentified Registered Entity 3		WECC201002257	PRC-005-1	1.1	High	
	Unidentified Registered Entity 4		WECC201002253	CIP-003-1	4.2	Lower[10]	
			WECC201002254	CIP-003-1	5.1	Lower	
			WECC201002258	CIP-004-1	2	Lower[11]	

[8] CIP-004-1 R3 has a "Medium" Violation Risk Factor (VRF); CIP-004-1 R3.1, R3.2 and R3.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the" Lower" VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[9] URE2 originally self-certified a violation of CIP-004-1 R4 but after reviewing the record, WECC's Compliance Enforcement Department concluded that the appropriate Standard in this case was CIP-006-1 R2 and not CIP-004-1 R4. WECC's Compliance Enforcement Department discussed the applicability of CIP-006-1 R2 to these facts with URE2, and URE2 agreed with WECC's Compliance Enforcement Department that the applicable Standard in this case is CIP-006-1 R2.

[10] CIP-003-1 R4 and R4.1 each have a "Medium" VRF; CIP-003-1 R4.2 and R4.3 each have a "Lower" VRF. When NERC first filed VRFs, it assigned CIP-003-1 R4 and R4.1 a "Lower" VRF. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRFs and on February 2, 2009 and August 20, 2009, the Commission approved the modified "Medium" VRFs for CIP-003-1 R4 and R4.1, respectively. Therefore, the "Lower" VRFs for CIP-003-1 R4 and R4.1 were in effect from June 18, 2007 until February 2, 2009 and June 18, 2007 through August 20, 2009 when the "Medium" VRFs for CIP-003-1 R4 and R4.1, respectively, became effective.

[11] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; CIP-004-1 R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			WECC201002259	CIP-004-1	4	Lower[12]	

Unidentified Registered Entity 1

WECC201002298 CIP-004-1 R3

The purpose statement of Reliability Standard CIP-004-1 provides in pertinent part:

> Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1 R3 provides:

> R3. Personnel Risk Assessment —The Responsible Entity[13] shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> > R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct

[12] 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.

[13] Within the text of Standard 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.

> more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
>
> R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
>
> R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

[Footnote added].

CIP-004-1 R3 has a "Medium" Violation Risk Factor (VRF) and a "N/A" Violation Severity Level (VSL).[14]

URE1 submitted a Self-Report to WECC reporting a violation of CIP-004-1 R3. URE1 discovered the violation two months prior during an internal review. URE1 discovered a single employee who did not have a PRA conducted within 30 days of being granted access to a URE1 control center. The employee had only physical, not cyber, access to the control center. The employee's access was revoked when the violation was discovered. Twenty-two days later, the employee's PRA was completed, and the employee's unescorted access to the control center was reinstated.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE1, through when URE1 revoked the employee's access.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, only one employee of URE1 did not have the PRA conducted prior to having access to CCAs and the employee only accessed the PSP and at no time did the employee access the CCA contained within that PSP.

[14] At the time of UREs' violations, CIP-002-1 through CIP-009-1 had Levels of Non-Compliance instead of VSLs. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

WECC201002406 CIP-006-1 R2

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

CIP-006-1 R2 provides:

> R2. 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.[15]

URE1 submitted a Self-Report to WECC reporting a violation of CIP-006-1 R2. URE1 stated that one of its janitors had a "hard key" to open a locked door from before the enforceable date of the Standard which the janitor had used repeatedly to gain access to a URE1 CCA. The janitor was not authorized to access the CCA.

[15] *See supra* n. 14.

WECC determined the duration of the violation to be from when the Standard became mandatory and enforceable for URE1, through when URE1 revoked the unauthorized access.

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, failure to implement operational and procedural controls to manage physical access to PSP, which occurred in this case, did allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to CCAs essential to the operation of the BPS, thereby potentially negatively impacting the BPS. The violation did not pose a serious or substantial risk to the BPS because URE1's CCAs have multiple layers of electronic security protection to prevent further intrusion and access to the controls.

WECC201002299 CIP-006-1 R3
CIP-006-1 R3 provides:

> R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:
>
> > R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
> >
> > R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

CIP-006-1 R3 has a "Medium" VRF and a "N/A" VSL.[16]

URE1 submitted a Self-Report to WECC reporting a violation of CIP-006-1 R3 stating it failed to implement appropriate responses to access control alarms. URE1 stated that three months prior, it

[16] *See supra* at n. 14.

identified that a number of recurring access control alarms had been activated at one of its CCAs and which had not been appropriately responded to. Specifically, URE1 identified over 100 alarms that were not appropriately accessed, responded to, and closed in accordance with URE1's physical security plan. In 73% of the identified alarm events, URE1 personnel failed to investigate and close alarms, but no unauthorized access to CCAs occurred; in 5% of the alarm events, unauthorized company employees accessed CCAs, but their activities were not malicious; in 8% of the alarm events, URE1 could not verify whether escorted or unescorted access was granted; and in 14% of the alarm events, URE1 was unable to identify the cause of the alarm or whether unauthorized access occurred.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable and URE1 failed to properly respond to the first alarm, through when URE1 completed its Mitigation Plan.[17]

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The individuals who gained unauthorized access to the CCAs in this case were employees working at the time of access. In these instances, while the alarms were not properly responded to, the alarms were monitored. Finally, URE1's CCAs have multiple layers of electronic security protection to prevent further intrusion and access to the controls.

WECC201002300 CIP-006-1 R4

CIP-006-1 R4 provides:

> R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
>
> > R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
> >
> > R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

[17] On April 1, 2010, CIP-006-1 R3 was replaced by CIP-006-2 R5 when CIP Version 2 went into effect. On October 1, 2010, CIP-006-2 R5 was replaced by CIP-006-3 R5, when CIP Version 3 went into effect.

> R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

CIP-006-1 R4 has a "Lower" VRF and a "N/A" VSL.[18]

URE1 submitted a Self-Report to WECC reporting a violation of CIP-006-1 R4 stating that three months prior, it discovered that access logs generated by some access points on its PSP did not contain sufficient level of detail to identify the individuals. Specifically, URE1 identified less than 50 instances where security personnel could not determine the person that accessed the PSP. URE1 stated that it reviewed access control alarms activated for a ten-month period.

WECC determined the duration of the violation to be from when the Standard became mandatory and enforceable for URE1, through when URE1 completed its Mitigation Plan.[19]

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, failure to log physical access at all access points to the PSP(s) could allow unauthorized access to go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets. Such access may then be used to cause harm to CCAs essential to the operation of the BPS. The violation did not pose a serious or substantial risk to the BPS because URE1's CCAs have multiple layers of electronic security protection to prevent further intrusion and access to the controls.

Unidentified Registered Entity 2

WECC201002379 CIP-006-1 R2

CIP-006-1 R2 has a "Medium" VRF and a "N/A" VSL.[20]

[18] *See supra* n. 14.
[19] On April 1, 2010, CIP-006-1 R4 was replaced by CIP-006-2 R6 when CIP Version 2 went into effect. On October 1, 2010, CIP-006-2 R6 was replaced by CIP-006-3 R5, when CIP Version 3 went into effect.
[20] *See supra* n. 14.

URE2 submitted a Self-Report[21] to WECC stating that three months prior, URE2 personnel identified a janitor entering a backup site for the generation management system which is a CCA at URE2's operations center. URE2 personnel reported the incident to URE2's compliance manager. URE2's compliance department performed a check to determine whether this janitor was authorized to have unescorted physical access to the PSP and determined that the janitor was not authorized to access the operations center. URE2 performed a review and identified over 100 individuals that had unauthorized access to the worksite. Those individuals were granted access in error resulting from a secondary database being used by URE2's physical card access system. The janitor gained access using a "hard key" which had been used prior to the enforceable date of the Standard, and which the janitor continued to use after the Standard became mandatory and enforceable.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2, through when URE2 reconfigured its operations center door access.[22]

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, failure to maintain a list of personnel with logical and/or physical access to CCAs could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to CCAs essential to the operation of the BPS. In this instance, the asset in scope is the backup site for generation management system. The personnel in scope only had physical access to the CCAs in scope. The risk was not serious or substantial because the CCAs in scope require username and password authentication, have 24x7 physical and electronic monitoring and logging, only those ports and services necessary are enabled, and have anti-virus and anti-malware software installed. In addition, the facility in scope has 24x7 video monitoring and usage of CCAs would be detected at the primary site.

[21] While the Settlement Agreement lists the discovery method as "Self-Report," URE2 self-reported this violation during its self-certification period and, because at the time of the Self-Report, URE2 had an existing obligation to self-certify to WECC whether it was compliant, it did not receive Self-Report credit in this case.
[22] On April 1, 2010, CIP-006-1 R2 was replaced by CIP-006-2 R4 when CIP Version 2 went into effect. On October 1, 2010, CIP-006-2 R4 was replaced by CIP-006-3 R4, when CIP Version 3 went into effect.

Unidentified Registered Entity 3

WECC201002257 PRC-005-1 R1.1

The purpose statement of Reliability Standard 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 R1.1 provides:

> R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:
>
> R1.1. Maintenance and testing intervals and their basis.

PRC-005-1 R1.1 has a "High" VRF and a "Lower" VSL.

URE3 submitted a Self-Report to WECC stating that for an eight-month period it had performed a refueling outage during which it replaced several obsolete electro-mechanical relays with digital protection relays. URE3's generation Protection System maintenance and testing program requires URE3 to establish maintenance and testing intervals for new protection equipment within 90 days of commissioning the equipment.

WECC determined the duration of the violation to be 90 days after URE3's newly installed relays were commissioned, through forty days later, when URE3 established maintenance and testing intervals for the installed relays.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, the protective relays in this case were new and tested upon their commissioning. Furthermore, the relays were not due for maintenance until two years later.

Unidentified Registered Entity 4

WECC201002253 CIP-003-1 R4.2

The purpose statement of Reliability Standard CIP-003-1 provides: "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 a part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R4.2 provides:

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

CIP-003-1 R4.2 has a "Lower" VRF and a "N/A" VSL.[23]

URE4 self-certified noncompliance with CIP-003-1 R4, stating that its CIP-related floor plans were provided to unauthorized third-party contractors. URE4 followed up its Self-Certification with a Self-Report clarifying the violation to be of CIP-003-1 R4.2. URE4's program for managing protected information associated with CCAs lacked a process for identifying and releasing protected information to third-party vendors. URE4 released protected information to eight unauthorized third-party vendors in a request for proposal process. During the contractor bid process, URE4 construction managers released the floor plans of a URE4 CIP facility to third-party contractors, as well as the winning bidder, without first identifying and protecting the information.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, through when URE4 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, failure to document and implement a program to ascertain and distinguish information related to CCAs could cause URE4 to be unaware of the content

[23] *See supra* n. 14.

and location of that information resulting in misuse by internal or external resources to gain access to CCAs. The violation did not pose a serious or substantial risk to the reliability of the BPS because there was no indication that the CIP protected information in this case was released in a malicious or suspicious manner. Instead, the recipients of the information, and the majority of potential future recipients, are past, existing, and potential UREs vendors who have good working relationships with UREs, or who seek to develop such relationships. The outside vendors who received the floor plans have cooperated with UREs in returning or destroying those floor plans.

WECC201002254 CIP-003-1 R5.1

CIP-003-1 R5.1 provides:

> R5. 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.

CIP-003-1 R5.1 has a "Lower" VRF and a "N/A" VSL.[24]

URE4 followed up its Self-Certification of the above CIP-003-1 R4.2 violation with a Self-Report that included an additional violation of CIP-003-1 R5.1.[25] URE4 stated that there is a documented program to manage access to protected information. This program includes a list of personnel with access to protected information, and the list is verified annually; however, during an internal review, URE4 found that a construction project manager's name was not included in URE4's lists of persons authorized to provide protected information. WECC's Compliance Enforcement Department further concluded that

[24] *See supra* n. 14.

[25] URE2 self-reported this violation during its Self-Certification period and, because at the time of the Self-Report, URE2 had an existing obligation to self-certify to WECC whether it was compliant, it did not receive Self-Report credit in this case.

URE4 was in violation of CIP-003-1 R5.1 because it did not identify the name and title of the construction manager, described in the R4.2 violation description that released CIP information to outside vendors, as well as did not identify the information for which the construction manager was responsible.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, through when URE4 completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, while failing to identify personnel responsible for authorizing access to CCA information and the information those personnel are responsible for could result in the improper release of CCA information, in this case the construction project manager was in fact responsible for the information that was released. The recipients of the information are past, existing, and potential UREs vendors who have good working relationships with UREs, or who seek to develop such relationships.

WECC201002258 CIP-004-1 R2
CIP-004-1 R2 provides:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
>
> R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> R2.2.1. The proper use of Critical Cyber Assets;
>
> R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

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

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

CIP-004-1 R2 has a "Lower" VRF and a "N/A" VSL.[26]

URE4 self-certified that two of its employees with access to CCAs were not trained within 90 days of being granted such access. URE4 followed-up its Self-Certification with a Self-Report. URE4 identified nine additional employees with access to CCAs who had not been trained within 90 days of being granted such access. The 11 individuals had not been trained because of an administrative oversight caused by the failure to have a central training database.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, through when URE4 completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Specifically, less than 1% of its personnel were not trained within 90 days of being granted physical access only to CCAs, and all of these personnel had current PRAs.

WECC201002259 CIP-004-1 R4
CIP-004-1 R4 provides:

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

[26] *See supra* n. 14.

> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" VRF and a "N/A" VSL.[27]

URE4 self-certified that it had failed to revoke access to CCAs within seven days for personnel who no longer required access to CCAs. URE4 followed-up its Self-Certification with a Self-Report. URE4 identified 11 individuals who should have had their access revoked because they no longer required access to the CCAs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, through when URE4 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, failure to revoke physical access to CCAs within seven calendar days could allow someone, using such access, to gain physical and potentially gain logical access to CCAs. This access may result in security compromise of the CCAs essential to the operation of the BPS. This violation did not pose a serious or substantial risk to the BPS because these personnel did have current PRAs and there is no indication that any of the employees engaged in any malicious or suspicious acts in connection with any CCAs.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred thirty-four thousand three hundred fifty dollars ($134,350) for the referenced violations. In reaching this determination, WECC considered the following factors: (1) UREs took voluntary corrective action to remediate the violations; (2) URE1 received self-reporting credit for four violations: WECC201002298, WECC201002406, WECC201002299 and WECC201002300;[28] (3) WECC reviewed UREs' internal compliance program (ICP) and considered it a mitigating factor in penalty determination; (4) UREs was cooperative throughout the process; (5) UREs did not fail to complete any applicable compliance

[27] *See supra* n. 14.

[28] URE2's CIP-006-1 R2, URE3's PRC-005-1 violation, and URE4's CIP-003-1 R5.1 and CIP-004-1 R4 violations were self-reported during the entities' Self-Certification period and, because at the time of the Self-Reports the entities had an existing obligation to self-certify to WECC whether they was complaint, they did not receive Self-Report credit for those violations.

directives; (6) There was no evidence of any attempt by UREs to conceal the violations; (7) There was no evidence that UREs' violations were intentional; (8) These are the first assessed violations of these standards by these Registered Entities; and (9) Although URE1 and URE2 both violated CIP-006-1 R2, WECC determined that aggravation for being affiliates and violating the same Reliability Standard was not warranted because the violations occurred contemporaneously and are factually similar. The conduct underlying both violations began prior to the compliance enforcement date and involved janitors making non-CIP-006 compliance entry into areas within Physical Security Perimeters with pre-existing "hard keys." Both of these violations were self-reported on the same date. WECC is not aware of any other UREs affiliates' violations of these Reliability Standards or involvement in UREs' activities such that these violations should be treated as recurring or repeated misconduct.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred thirty-four thousand three hundred fifty dollars ($134,350) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[29]

Unidentified Registered Entity 1

WECC201002298 CIP-004-1 R3
URE1's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to WECC on May 27, 2010 stating it had been completed on May 21, 2010. The Mitigation Plan was accepted by WECC on November 17, 2010 and approved by NERC on December 15, 2010. The Mitigation Plan for this violation is designated as MIT-10-3148 and was submitted as non-public information to FERC on December 17, 2010 in accordance with FERC orders.

URE1's Mitigation Plan stated that URE1 had:

1. Immediately revoked the employee's access and notified local management to provide an appropriate escort;
2. The employee's PRA was completed and unescorted access was reinstated;
3. Revised UREs' CIP-004 procedure document to add the requirement that PRA coordinators perform visual inspections of all PRA evidence and secure that evidence prior to adding the individual's name to the master PRA list; and

[29] *See* 18 C.F.R § 39.7(d)(7).

4. Revised the document's performance of quarterly assessment outline of the master PRA list to align with the requirements outlined in CIP-004 R4.1 which addresses quarterly review of an entity's CCA access list.

URE1 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE1 submitted the following:

1. Evidence that a PRA was conducted for the person in scope; and
2. The revised procedure document, to ensure manual confirmation of a PRA is completed prior to updating the access list.

After reviewing URE1's submitted evidence, WECC verified that URE1's Mitigation Plan was completed.

WECC201002406 CIP-006-1 R2

URE1's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC on March 16, 2011 stating it had been completed on October 28, 2010. The Mitigation Plan was accepted by WECC on June 6, 2011 and approved by NERC on July 11, 2011. The Mitigation Plan for this violation is designated as MIT-10-3822 and was submitted as non-public information to FERC on July 14, 2011 in accordance with FERC orders.

URE1's Mitigation Plan for its violation of CIP-006-1 R2 stated that the actions taken pursuant to the Mitigation Plan submitted for CIP-006-1 R3 and R4 (MIT-10-3149 discussed in detail below) appropriately mitigated the violation of CIP-006-1 R2.

URE1 certified that the above Mitigation Plan requirements were completed.

After reviewing URE1's submitted evidence, WECC verified that URE1's Mitigation Plan was completed.

WECC201002299 CIP-006-1 R3 and WECC201002300 CIP-006-1 R4

URE1's Mitigation Plan to address its violations of CIP-006-1 R3 and R4 was submitted to WECC on April 27, 2010 with a proposed completion date of October 31, 2010. The Mitigation Plan was accepted by WECC on November 17, 2010 and approved by NERC on December 15, 2010. The Mitigation Plan for these violations is designated as MIT-10-3149 and was submitted as non-public information to FERC on December 17, 2010 in accordance with FERC orders.

URE1's Mitigation Plan required URE1 to:

1. Initiate vulnerability and configuration assessments of all CCA facilities per CIP-007 guidelines and compare that information to its most recent baseline assessments;
2. Inspect, evaluate and test PSP protection equipment of all CCA facilities for proper operation and functionality;
3. Inspect all affected facilities for possible signs of adverse activity;
4. Instruct the janitorial service personnel not to enter the affected facilities and confiscated their access keys. Locks were re-keyed at these facilities. Proper signage has been posted on PSP access points. The remaining CCA facilities have been re-keyed;
5. Re-evaluate and redefine certain security positions responsible for responding to NERC-related alarms, and elevate the position classification and required skills. Additional staff has been retained, trained and are on duty;
6. Enhance its alarm response process with respect to protocols for appropriately assessing, responding, and positively closing access control alarms;
7. Develop an alarm response training program to educate employees on access control alarm response. URE1 has developed additional training for all access control response personnel requiring a written exam;
8. Post signs at access points instructing employees to follow the access control alarm procedure; and
9. Review the access control procedures and the developed physical security plan to assure strict compliance with CIP-006.

URE1 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE1 submitted the following:

1. Evidence that URE1 conducted a vulnerability and configuration assessment at all facilities;
2. Evidence that URE1 inspected, evaluated and tested physical security protection;
3. Access control procedures;
4. Alarm response procedures; and
5. Alarm response training program and evidence employees were trained.

After reviewing URE1's submitted evidence, WECC verified that URE1's Mitigation Plan was completed.

Unidentified Registered Entity 2

WECC201002379 CIP-006-1 R2

URE2's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC on March 2, 2011[30] with a proposed completion date of April 30, 2011. The Mitigation Plan was accepted by WECC on March 11, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan for this violation is designated as MIT-10-3527 and was submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE2's Mitigation Plan required URE2 to:

1. Reconfigure operations center door access in URE2's access control monitoring system to remove access privileges from employees not on the authorized access list for NERC restricted areas;
2. Refine access control monitoring system configuration change management process and procedures to assure strict compliance with CIP-006; and
3. Activate URE2's anti-vulnerability emergency response team to evaluate security of the CCAs within the Electronic Security Perimeter to ensure no malicious or suspicious activity had taken place at the operations center.

URE2 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE2 submitted the following:

1. Two documents have been developed to record the processes that corporate security must follow when deciding that a configuration change to an access control monitoring system is required.
2. Two documents have been developed to record the procedures that corporate security must follow when deciding that a configuration change to an access control monitoring system is required.

[30] URE2 submitted a Mitigation Plan on August 11, 2010 to mitigate its then-perceived CIP-004-1 R4 violation. After WECC concluded that this was actually a violation of CIP-006-1 R2, URE2 submitted a revised Mitigation Plan.

3. URE2 also relabeled the mislabeled card reader and updated the map where the card reader is shown. URE2 then communicated this change to the impacted personnel. The documents show the changed map, change history and email communicating the change.

After reviewing URE2's submitted evidence, WECC verified that URE2's Mitigation Plan was completed.

Unidentified Registered Entity 3

WECC201002257 PRC-005-1 R1.1
URE3's Mitigation Plan to address its violation of PRC-005-1 R1.1 was submitted to WECC on September 29, 2010 with a proposed completion date of November 30, 2010. The Mitigation Plan was accepted by WECC on October 29, 2010 and approved by NERC on November 24, 2010. The Mitigation Plan for this violation is designated as MIT-10-3070 and was submitted as non-public information to FERC on November 24, 2010 in accordance with FERC orders.

URE3's Mitigation Plan required:

1. URE3 to establish the maintenance and testing intervals for the new protection relays;
2. URE3's engineering group to conduct an evaluation to determine and address the issue; and
3. URE3's design engineering group to revise the engineering change procedure to clarify protocols for compliance with NERC Reliability Standards.

URE3 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE3 submitted the following:

1. Maintenance and testing intervals for new relays;
2. URE3's revised design engineering change procedure; and
3. URE3's Protection System design engineers required reading assignment and electronic tracking document.

After reviewing URE3's submitted evidence, WECC verified that URE3's Mitigation Plan was completed.

Unidentified Registered Entity 4

WECC201002253 CIP-003-1 R4.2 and WECC201002254 CIP-003-1 R5.1

URE4's Mitigation Plan to address its violations of CIP-003-1 R4.2 and R5.1 was submitted to WECC on May 28, 2010 with a proposed completion date of August 31, 2010. The Mitigation Plan was accepted by WECC on November 11, 2010 and approved by NERC on December 13, 2010. The Mitigation Plan for these violations is designated as MIT-09-3118 and was submitted as non-public information to FERC on December 14, 2010 in accordance with FERC orders.

URE4's Mitigation Plan required URE4 to:

1. Require the vendors who improperly received CCA information to destroy that information;
2. Update its CCA information protection program; and
3. Train employees on the process for releasing CCA information.

URE4 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE4 submitted the following:

1. List for protected information;
2. Revised approver list; and
3. Evidence URE4 trained employees regarding changes to its information protection program.

After reviewing URE4's submitted evidence, WECC verified that URE4's Mitigation Plan was completed.

WECC201002258 CIP-004-1 R2

URE4's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted to WECC on May 28, 2010 with a proposed completion date of August 31, 2010. The Mitigation Plan was accepted by WECC on February 8, 2011 and approved by NERC on March 7, 2011. The Mitigation Plan for this violation is designated as MIT-09-3388 and was submitted as non-public information to FERC on March 10, 2011 in accordance with FERC orders.

URE4's Mitigation Plan required URE4 to:

1. Confirm employee need for access with management;
2. Request employee completion of NERC CIP training for some employees;

3. Revoke access for remaining employees; and
4. Continue operating existing data reconciliation program to confirm that URE4's access lists contain the names of all URE4 employees with electronic or physical access to CCAs.

URE4 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE4 submitted the following:

1. Training records and status, revocation, updated procedures, reinforcement training materials, mitigation plan report and process for remediation; and
2. Access list sample.

After reviewing URE4's submitted evidence, WECC verified that URE4's Mitigation Plan was completed.

WECC201002259 CIP-004-1 R4

URE4's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to WECC on May 28, 2010 with a proposed completion date of August 31, 2010. The Mitigation Plan was accepted by WECC on January 4, 2011 and approved by NERC on January 26, 2011. The Mitigation Plan for this violation is designated as MIT-09-3246 and was submitted as non-public information to FERC on January 27, 2011 in accordance with FERC orders.

URE4's Mitigation Plan required URE4 to:

1. Confirm employee need for access with management;
2. Request employee completion of NERC CIP training for three employees;
3. Revoke access for remaining employees; and
4. Continue operating existing data reconciliation program to confirm that URE4's access lists contain the names of all URE4 employees with electronic or physical access to CCAs.

URE4 certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE4 submitted the following:

1. Training records and status, revocation, updated procedures, reinforcement training materials, mitigation plan report and process for remediation; and
2. Access list sample.

After reviewing URE4's submitted evidence, WECC verified that URE4's Mitigation Plan was completed.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[32] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on March 12, 2012. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred thirty-four thousand three hundred fifty dollar ($134,350) financial penalty against UREs and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. The violations constituted UREs' first occurrence of violations of the subject NERC Reliability Standards;
2. UREs self-reported the following violations: WECC201002298, WECC201002406, WECC201002299 and WECC201002300;
3. WECC reported that UREs was cooperative throughout the compliance enforcement process;
4. UREs had a compliance program at the time of the violations which WECC considered a mitigating factor, as discussed above;
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

[31] *See* 18 C.F.R. § 39.7(d)(4).
[32] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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-four thousand three hundred fifty dollars ($134,350) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between WECC and UREs, included as Attachment a;

b) Record documents for the violation of WECC201002298 CIP-004-1 R3, included as Attachment b:

1. URE1's Source Document;
2. URE1's Mitigation Plan;
3. URE1's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of WECC201002406 CIP-006-1 R2, included as Attachment c:

1. URE1's Source Document;
2. URE1's Mitigation Plan
3. URE1's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of WECC201002299 CIP-006-1 R3 and WECC201002300 CIP-006-1 R4, included as Attachment d:

1. URE1's Source Document;
2. URE1's Mitigation Plan;
3. URE1's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

e) Record documents for the violation of WECC201002379 CIP-006-1 R2, included as Attachment e:

1. URE2's Source Document;
2. URE2's Mitigation Plan;
3. URE2's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

f) Record documents for the violation of WECC201002257 PRC-005-1 R1.1, included as Attachment f:

1. URE3's Source Document;
2. URE3's Mitigation Plan
3. URE3's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for the violation of WECC201002253 CIP-003-1 R4.2 and WECC201002254 CIP-003-1 R5.1, included as Attachment g:

1. URE4's Source Document for CIP-003-1 R4;
2. URE4's Source Document for CIP-003-1 R4.2 and R5.1;
3. URE4's Mitigation Plan;
4. URE4's Certification of Mitigation Plan Completion;
5. WECC's Verification of Mitigation Plan Completion;
6. WECC's Verification of Mitigation Plan Completion for CIP-003-1 R5.1;

h) Record documents for the violation of WECC201002258 CIP-004-1 R2, included as Attachment h:

1. URE4's Source Document;
2. URE4's Mitigation Plan;
3. URE4's Certification of Mitigation Plan Completion
4. WECC's Verification of Mitigation Plan Completion;

i) Record documents for the violation of WECC201002259 CIP-004-1 R4, included as Attachment i:

1. URE4's Source Document;
2. URE4's Mitigation Plan;
3. URE4's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[33]

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

[33] *See* 18 C.F.R § 39.7(d)(6).

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charlie.berardesco@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 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net 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 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

	*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

cc: UREs
Western Electricity Coordinating Council

Attachments