PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

February 28, 2013

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, and Unidentified Registered Entity 3, FERC Docket No. NP13-_-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, and Unidentified Registered Entity 1 (URE3), NERC Registry ID# NCRXXXXX, (collectively, URE), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (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 CIP-006-1 R3.1 by URE1; CIP-004-3 R3.2, CIP-006-1 R1.6, R3 and R4 by URE2; and CIP-007-1 R1, R3, R5.3.2 and CIP-007-2 R6 by URE3. 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 fifty-one thousand five hundred dollars ($151,500), in addition to other remedies and actions to mitigate the instant violations and facilitate future

[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.

compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201102712 for URE1; WECC201102660, WECC201002653, WECC201102651 and WECC201102798 for URE2; and WECC201102671, WECC201002672, WECC201102799 and WECC201002673 for URE3 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 April 5, 2012, 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 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity Acronym	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	URE1	NOC-1333	WECC201102712	CIP-006-1	3.1	Medium[4]	$151, 500
	URE2		WECC201102660	CIP-004-3	3.2	Lower[5]	
			WECC201002653	CIP-006-1	1.6	Medium[6]	

[4] CIP -006-1 R3 and R3.1 each have a Medium VRF and R3.2 has a Lower VRF.
[5] CIP-004-1 R3 has a Medium VRF; 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. The VRFs for CIP-004-3 R3 were not changed when CIP-004-3 went into effect on October 1, 2010.
[6] When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from July 1, 2008 until February 2, 2009 when the Medium VRF became effective. CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 are each assigned a Medium VRF and CIP-006-1 R1.7, R1.8 and R1.9 are each assigned Lower VRF.

			WECC201102651	CIP-006-1	3	Medium	
			WECC201102798	CIP-006-1	4	Lower	
	URE3		WECC201102671	CIP-007-1	1	Medium[7]	
			WECC201002672	CIP-007-1	3	Lower	
			WECC201102799	CIP-007-2	6	Medium[8]	
			WECC201002673	CIP-007-1	5.3.2	Lower[9]	

Unidentified Registered Entity 1

WECC201102712 CIP-006-1 R3

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

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

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

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

CIP-006-1 R3 provides:

> R3. Monitoring Physical Access — The Responsible Entity[10] 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.

[Footnote added.]

CIP-006-1 R3 has a "Medium" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL).

URE1 submitted a Self-Report to WECC stating that it had failed to provide alarming for five card readers that controlled access to three Physical Security Perimeters (PSPs) in violation of CIP-006-1 R3. Four of the card readers controlled access to the blackstart human machine interface (HMI) PSP at two of URE1's facilities. The card readers involved were incorrectly configured and failed to send alarms to the central alarm station. In addition, one card reader's air compressor PSP card reader was unplugged from its power source which caused the reader to fail to send an alarm to the central alarm station.

URE1 submitted an additional Self-Report stating that there were four instances where the controls for the monitoring of PSPs were not implemented. The first instance involved the first facility programmable logic controller (PLC) cabinet PSP housing gas compressors. The second instance involved the PSP at second facility PLC cabinet, which also houses gas compressors. Both of these PSPs did not have the controls implemented for monitoring physical access.

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

The third instance involved a PLC cabinet PSP at the third power plant, which houses an ammonia vaporizer heater which is a Critical Cyber Asset (CCA) used in generation. A technician performed repairs on a CCA within the PSP and did not re-arm the card reader upon exit, thereby deactivating the cabinet's real-time central alarm monitoring for a period of two hours and 32 minutes.

Finally, the fourth instance involved a PLC cabinet PSP for the Gas Compressor at the second facility, which houses a CCA used in generation. A technician performed repairs on a CCA within the PSP and did not re-arm the card reader upon exit, thereby deactivating the cabinet's real-time central alarm monitoring for a period of two hours and 52 minutes.

WECC determined that URE1 was in violation of CIP-006-1 R3 for failing to implement technical and procedural controls for monitoring physical access at all access points to the PSP twenty-four hours a day.

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

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, failure to monitor physical access at all access points to the PSPs could allow unauthorized access to a PSP to go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets. As compensating measures, URE1 stated that it has 24 hours a day, seven days a week logging of physical access and 24 hours a day, seven days a week logging and monitoring of electronic access of the PSPs and Electronic Security Perimeters (ESPs) in scope, all CCAs in scope require usernames and passwords, card readers at the HMI PSPs were controlling physical access, and the air compressor PSP was locked with key access to a limited number of authorized personnel.

Unidentified Registered Entity 2

WECC201102660 CIP-004-3 R3.2
The purpose statement of Reliability Standard CIP-004-3 provides:

> Standard CIP-004-3 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-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

CIP-004-3 R3 provides:

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

CIP-004-3 R3.2 has a "Lower" VRF and a "Moderate" VSL.

URE2 submitted a Self-Report to WECC stating that it had failed to update the personnel risk assessment (PRA) for one of its employees. URE2 further stated that the employee's PRA was valid until it expired in the fall. URE2 discovered the expired PRA during a quarterly PRA review, resubmitted the PRA, and approximately a month later completed the PRA for the employee.

WECC determined the duration of the violation to be from when URE2 should have performed the PRA through when URE2 performed the PRA.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS because the employee had physical access to only one CCA within the PSP which was used as a part of URE2's management system. The CCA had electronic access, logging and monitoring controls. The room containing the CCA has at least three operators at all times. In the event the employee had misconfigured the generation management threshold, additional alerts would have reported the misconfiguration to URE2 operators.

WECC201002653 CIP-006-1 R1.6
CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> *****
>
> R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

CIP-006-1 R1.6 has a "Medium" VRF and a "Moderate" VSL.

URE2 submitted a Self-Certification to WECC stating that on five instances, visitors were not escorted at all times while visiting one of URE2's PSPs. The first instance occurred when visitors were unescorted for five to ten minutes. The visitors were Information Technology (IT) department employees escorted into the PSP to install a laptop computer. The escort left the visitors unattended for a brief period to escort in other IT personnel. Within minutes of the escort leaving, a manager discovered the unescorted visitors and remained with the visitors until the escort returned. There was no indication of any suspicious activity or attempt to harm any CCAs.

The second instance occurred when URE2 failed to provide continuous escorted access to three employees when they were inside the PSP. A security officer escorted three employee workers where they needed to drop off some materials in the PSP prior to exiting the facility. The security officer briefly left the contingent workers to escort in an additional two other persons waiting outside the PSP. When the employee that received the delivery realized the workers were unescorted, the employee that received the delivery escorted them out of the PSP. Additionally, corporate security realized the workers should have remained escorted by the original employee throughout the delivery and immediately dispatched two other security officers to escort the three workers out of the PSP.

Corporate security questioned the workers and confirmed that, upon completing their task, the workers had departed the PSP to exit the facility, were escorted by the employee that received the delivery, and had not done anything that would pose a threat to the CCA.

The third instance occurred when URE2 failed to provide continuous escorted access to four visitors to a PSP for five to ten minutes. An employee escorted four summer law clerks into a PSP for a tour. The escort left the clerks with the employee giving the tour for approximately 10 minutes. The employee giving the tour has authorized access to the CCA and remained with the clerks at all times until the escort returned. However, URE2 procedures at the time did not allow the original escort to "hand-off" the visitors to another escort without first recording that fact on the CIP visitor log.

The fourth instance occurred when URE2 failed to provide continuous escorted access to three visitors to a PSP for five to ten minutes. An employee escorted three visitors to a meeting in a conference room within a PSP. Midway through the meeting, one of the visitors needed to leave the secured area, and the escort walked with the departing visitor to exit the PSP, leaving the other two visitors in the conference room. Other participants in the meeting were with the other two visitors for the duration of the escort's absence and they confirmed the two visitors remained in the conference room and did not attempt to approach the CCA while the escort was out of the room.

The fifth instance occurred when an employee failed to follow established physical access controls and was able to access a PSP by using another employee's ID card. The employee has authorized unescorted access to gain access to an area secured pursuant to NERC CIP Standards. The employee used the ID card of another individual, with identical access rights, because the employee forgot the required ID. In such a case, URE2's procedures require employees to sign-in on a physical log for each entry when they do not have their ID in their possession, and the procedures also prohibit individuals from using an ID card that does not belong to them.

WECC determined the duration of the violation to be five instances which occurred during a six month period.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS because the unescorted accesses were to only one CCA within the PSP which was used as part of URE2's management system. The CCA had electronic access, logging and monitoring controls. The room containing the CCA has at least three operators at all times. In the event generation management threshold was misconfigured, additional alerts would have reported the misconfiguration to the URE2's operators.

WECC201102651 CIP-006-1 R3
CIP-006-1 R3 has a "Medium" VRF and a "Severe" VSL.

URE2 submitted a Self-Report to WECC stating that alarms generated at one access point to the PSP were not monitored or reviewed. The alarms at the access point were not monitored or reviewed because of an unintentional change made by an operator that led to configuration changes to alarm systems. Specifically, the change prevented alarm events from being displayed on security monitors and, consequently, URE2's security personnel were unable to immediately review alarm events associated with unauthorized access. After URE2 discovered the improper configuration, it conducted a review of all alarms generated since the unintentional change by the operator was made and determined that two alarm events were not reviewed by security personnel.

WECC determined the duration of the violation to be on two occasions: the dates the two alarms were not immediately handled as required by CIP-006-1 R3.

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 monitor physical access at all access points to the PSP could allow unauthorized access to the PSP 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, thereby potentially negatively impacting the BPS. The risk to the reliability of the BPS was not serious or substantial because the CCA had electronic access, logging and monitoring controls. The room containing the CCA has at least three operators at all times. In the event generation management threshold was misconfigured, additional alerts would have reported the misconfiguration to the entity's operators.

WECC201102798 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.

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 "High" VSL.

URE2 submitted a Self-Report to WECC stating that a software misconfiguration caused alarms generated from a PSP to not be sent to the central alarm station, which resulted in inaccurate logging of employees' access to the PSP. In its Self-Report, URE2 describes that to access the facility the PSP is protecting without generating an alarm, an employee must use an ID card and also use a hard key. However, an employee can access the PSP using only a hard key. When an employee accesses the PSP using only a hard key, an alarm is generated. When the system is functioning properly, the individual responsible for responding to alarms on the PSP, logs the employee that accessed the PSP, as using only a hard key.

Due to a configuration change, alarm events were not sent to the central alarm station and, as a result, did not appear on security monitors. Because the alarm events did not appear on security monitors, the individual responsible for responding to alarm events was unaware of the alarms and did not log the employee who accessed the PSP using only hard keys.

WECC determined the duration of the violation to be from when URE2 misconfigured its system through when URE2 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 the access point protected one CCA used for the management system. As compensating measures, URE2 stated that the only CCAs located at this PSP had electronic access, logging and monitoring controls. In the event someone with a hard key accessed the PSP and misconfigured the generation management threshold, additional detection controls would have detected and reported the misconfiguration to the entity's operators.

Unidentified Registered Entity 3

WECC201102671 CIP-007-1 R1

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

CIP-007-1 R1 provides:

> The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):
>
> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> > R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
> >
> > R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
> >
> > R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF[11] and a "Severe" VSL.

URE3 submitted a Self-Certification to WECC stating that in 14 instances, URE3 did test for adverse effects prior to implementing changes to 80 or more existing Cyber Assets within the ESP, but URE3 did

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

not document the test results before implementing the changes. Also, URE3 stated that, in two instances, URE3 did not test for adverse effects prior to implementing changes. All of these 16 instances are contrary to URE3's CIP-007 procedures, which require URE3 to test, document, and implement changes to its Cyber Assets.

WECC determined the duration of the violation to be from when the first change was implemented through when URE3 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 follow URE3's cyber security test procedures for the Cyber Assets within an ESP could allow untested and potentially malicious changes (*e.g.* patch, service pack, vendor release, application or database update *etc*.) to be released in the production systems. Such issues could expose cyber security vulnerabilities into the CCAs essential to the operation of the BPS. If exposed, such vulnerabilities could negatively impact the normal operation of the BPS. URE3's transmission systems for its higher voltage lines spans approximately 5,000 transmission circuit miles. As a compensating measure, URE3 stated the devices were located within a PSP and an ESP, and thus, were afforded the protections specified in CIP-005 and CIP-006. More specifically, the following CIP-005 protections were in place: access points were protected; electronic access controls were in place; there was monitoring of electronic assets; and there was documentation and review of maintenance. With respect to CIP-006 protections, the following protections were in place: there was physical protection of physical access control systems; electronic access control; monitoring of physical access, logging of physical access; and there was maintenance and testing.

WECC201002672 CIP-007-1 R3

CIP-007-1 R3 provides:

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

URE3 submitted a Self-Certification to WECC stating that it failed to assess security patches within 30 days of the patches being made available. There were a total of 196 security patches on six devices that were not assessed within 30 days of being made available. The devices were located in two ESPs.

WECC determined the duration of the violation to be the longest time period a security patch was made available, but was not assessed as required by the Standard. The duration of the violation was for approximately one year.

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 assess security patches could result in vulnerabilities remaining unaddressed for extended periods of time. This increases the risk of a successful cyber attack against CCAs essential to the operation of the BPS. URE3's transmission systems for its higher voltage lines spans approximately 5,000transmission circuit miles. As compensating measures, URE3 stated that the devices in scope had file integrity checking tools, intrusion prevention systems, dual-factor authentication, and all personnel with access to these systems completed training and had a PRA.

WECC201102799 CIP-007-2 R6

The purpose statement for CIP-007-2 provides:

> Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

CIP-007-2 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement

automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. 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.

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-008-2.

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-007-2 R6 has a "Medium" VRF and a "Severe" VSL.

URE3 submitted a Self-Certification to WECC stating that two servers within an ESP were installed but were not configured to send Syslogs, a standard for computer data logging, to URE3's Syslog server as specified in URE3's CIP-007-1 R6 process. The two servers that were installed and are used as primary and back-up real-time providers of supervisory control and data acquisition (SCADA) information. Since the devices were not configured to send Syslogs, the logs were not reviewed or retained as required by the Standard.

WECC determined the duration of the violation to be from when the devices were installed through when URE3 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 implement security controls to monitor cyber security system events 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, thereby potentially negatively impacting the

BPS. URE3's transmission systems for its higher voltage lines spans approximately 5,000 transmission circuit miles. In addition, the devices in scope were not afforded the protections specified in CIP-007 R6. The servers in scope are used as a primary and back-up for providing real-time SCADA data. As compensating measures, URE3 stated the devices in scope were in a PSP and ESP, and thus afforded many of the protections specified in CIP-005 and CIP-006.

WECC201002673 CIP-007-1 R5.3.2

CIP-007-1 R5.3.2 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> *****
>
> R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
>
> *****
>
> R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

CIP-007-1 R5.3.2 has a "Lower" VRF and a "Lower" VSL.

URE3 submitted a Self-Certification to WECC stating that it did not ensure that its passwords were changed at least annually for five individuals in violation of CIP-007-1 R5.3.3. WECC determined that URE3 did in fact change the passwords for the five individuals annually. It was discovered that two of the five individuals did not have "complex" passwords, as required by CIP-007-1 R5.3.2. Two of URE3's employees' passwords did not contain a combination of alpha, numeric, and "special" characters.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE3 through when URE3 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 the devices in scope were in a PSP and ESP and were afforded the protections specified in CIP-005 and CIP-006.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty-one thousand five hundred dollars ($151,500) for the referenced violations. In reaching this determination, WECC considered the following factors: (1) the VRF and VSL; (2) URE took voluntary corrective action to remediate the violations of WECC201102712 by URE1, WECC201102660, WECC201102651 and WECC201102798 by URE2, and WECC201002672 by URE3; (3) URE self-reported the violations of WECC201102712 by URE1, WECC201102660, WECC201102651 and WECC201102798 by URE2, and WECC201102672 by URE3; (4) the quality of the URE's compliance program; (5) WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS; (6) URE's compliance history; (7) URE was cooperative throughout the process; (8) URE did not fail to complete any applicable compliance directives; (9) There was no evidence of any attempt by URE to conceal the violations; (10) There was no evidence that URE's violations were intentional; and (11) WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred fifty-one thousand five hundred dollars ($151,500) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[12]

Unidentified Registered Entity 1

WECC201102712 CIP-006-1 R3.1

URE1's Mitigation Plan to address its violation of CIP-006-1 R3.1 was submitted to WECC, and a revised Mitigation Plan was submitted to WECC approximately two months later. URE1 also submitted a Mitigation Plan extension request. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3807 and was submitted as non-public information to FERC in accordance with FERC orders.

[12] *See* 18 C.F.R § 39.7(d)(7).

URE1's Mitigation Plan stated that URE1 took the following actions to mitigate the violation:

1. Although there is no evidence of malicious PSP or ESP breach, URE1 initiated Anti-Vulnerability Emergency Response Team (AVERT) to evaluate the security of the CCAs within the ESP at two facilities;
2. URE1 reconfigured its access control monitoring system to add "Forced" and "Held" alarms at the two facilities;
3. URE1 performed log assessment and review for the two facilities;
4. URE1 refined the CCURE System configuration change management process and procedures to assure strict compliance with CIP-006;[13]
5. URE1 modified test and maintenance documentation to include annual testing; and
6. URE1 conducted quarterly testing of URE1 PSPs, for two quarters.

URE1's Amended Mitigation Plan added the additional activities URE1 would take to mitigate the violations:

1. Implement an administrative control which will require a formal "Work Authorization" for entry into CIP PSPs;
2. Review engineering design and construction of security monitoring devices for card readers installed in cabinets; and
3. Continue Quarterly Testing of URE1- PSPs for two additional quarters.

URE1 certified that the above Mitigation Plan requirements were completed. URE1 submitted evidence of completion of its Mitigation Plan to WECC.

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

Unidentified Registered Entity 2

WECC201102660 CIP-004-3 R3.2
URE2's Mitigation Plan to address its violation of CIP-004-3 R3.2 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation

[13] CCURE is a scalable security management solution encompassing complete access control and advanced event monitoring.

Plan for this violation is designated as MIT-11-3804 and was submitted as non-public information to FERC in accordance with FERC orders.

URE2's Mitigation Plan stated URE2 had taken the following actions to mitigate the violation:

1. URE2 performed a PRA for the employee involved;
2. PRA coordinators were trained to compare the name on the PRA questionnaire and Master PRA list to the name that is entered in the vendors system prior to submitting the PRA;
3. PRA coordinators are now required to be especially attentive to potential name, personnel number, date of birth, and social security discrepancies when reviewing completed PRAs; and
4. URE corporate security management conducted training for all personnel responsible for submitting or reviewing PRAs and reviewing the results.

URE2 certified that the above Mitigation Plan requirements were completed. URE2 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201002653 CIP-006-1 R1.6
URE2's Mitigation Plan to address its violation of CIP-006-1 R1.6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005170 and was submitted as non-public information to FERC in accordance with FERC orders.

URE2's Mitigation Plan required URE2 to:

1. Counsel the employees involved in the violation on the correct CIP-006-1 R1 procedures;
2. Suspend the contractor's access and provide NERC training; and
3. Reinforce previously provided training to all employees with physical access to PSPs.

URE2 certified that the above Mitigation Plan requirements were completed. URE2 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201102651 CIP-006-1 R3

URE2's Mitigation Plan to address its violation of CIP-006-1 R3[14] was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3760 and was submitted as non-public information to FERC in accordance with FERC orders.

URE2's Mitigation Plan stated URE2 had taken the following actions to mitigate the violation:

1. Reconfigured its alarm system and put in place privilege controls to prevent recurrence of the improper configuration;
2. Refined the CCURE System configuration change management process and procedures;
3. Performed log assessments for URE2 CCAs;
4. Initiated AVERT to evaluate the security of CCAs within the ESP;
5. Modified test and maintenance documentation to include annual testing; and
6. Performed test and maintenance activities for all URE2 sites.

URE2 certified that the above Mitigation Plan requirements were completed. URE2 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201102798 CIP-006-1 R4

URE2's Mitigation Plan to address its violation of CIP-006-1 R4[15] was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-11-3860 and was submitted as non-public information to FERC in accordance with FERC orders.

URE2's Mitigation Plan required URE2 to:

1. Reconfigure its access control and monitoring system to add events for the central alarm system NERC desk;
2. Refine its CCURE system configuration change management process and procedures to ensure strict compliance with the Standard;

[14] The Mitigation Plan was submitted originally for CIP-006-1 R5.
[15] The Mitigation Plan was submitted originally for CIP-006-1 R5.

3. Log assessments;
4. Initiated AVERT to evaluate the security of CCAs within the ESP;
5. Modified test and maintenance documentation to include annual testing; and
6. Performed test and maintenance activities for all URE2 sites.

URE2 certified that the above Mitigation Plan requirements were completed. URE2 submitted evidence of completion of its Mitigation Plan to WECC.

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

Unidentified Registered Entity 3

WECC201102671 CIP-007-1 R1
URE3's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005630 and was submitted as non-public information to FERC in accordance with FERC orders.

URE3's Mitigation Plan required URE3 to:

1. Have all changes reviewed by an advisory board;
2. Enhance its Request for Change tracking log;
3. Develop a weekly report listing all Requests for Change; and
4. Assign an IT quality assurance analyst to participate in advisory board meetings.

URE3 certified that the above Mitigation Plan requirements were completed. URE3 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201002672 CIP-007-1 R3
URE3's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as MIT-10-3755 and was submitted as non-public information to FERC in accordance with FERC orders.

URE3's Mitigation Plan required URE3 to:

1. Assess the applicability of all security patches made available to its Critical Assets;
2. Dedicate a Power Systems Control subject matter expert to tracking patch availability;
3. Enhance patch tracking to better clarify roles and responsibilities, as well as dates of patch availability and assessment; and
4. Create a review board that meets twice a month.

URE3 certified that the above Mitigation Plan requirements were completed. URE3 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201102799 CIP-007-2 R6

URE3's Mitigation Plan to address its violation of CIP-007-2 R6 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005631 and was submitted as non-public information to FERC in accordance with FERC orders.

URE3's Mitigation Plan required URE3 to:

1. Enable the Syslog function for the two servers at issue; and
2. URE3's IT Department created an IT NERC CIP Implementation Checklist.

URE3 certified that the above Mitigation Plan requirements were completed. URE3 submitted evidence of completion of its Mitigation Plan to WECC.

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

WECC201002673 CIP-007-1 R5.3.2

URE3's Mitigation Plan to address its violation of CIP-007-1 R5.3.2 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005391 and was submitted as non-public information to FERC in accordance with FERC orders.

URE3's Mitigation Plan required URE3 to:

1. Change the passwords of the individuals involved in the violation; and
2. Implement a procedure to ensure that its advisory board is notified of password changes.

URE3 certified that the above Mitigation Plan requirements were completed. URE3 submitted evidence of completion of its Mitigation Plan to WECC.

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[16]

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,[17] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 10, 2012. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifty-one thousand five hundred dollar ($151,500) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE's compliance history;
2. URE took voluntary corrective action to remediate the violations of WECC201102712 by URE1; WECC201102660, WECC201102651 and WECC201102798 by URE2; and WECC201002672 by URE3;
3. URE self-reported the violations of WECC201102712 by URE1; WECC201102660, WECC201102651 and WECC201102798 by URE2; and WECC201102671 by URE3;

[16] *See* 18 C.F.R. § 39.7(d)(4).
[17] *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).

4. WECC reported that URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed above;
6. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. There was no evidence that URE's violations were intentional;
8. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
9. URE did not fail to complete any applicable compliance directives; and
10. 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 fifty-one thousand five hundred dollars ($151,500) 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 URE executed April 5, 2012, included as Attachment a;

b) Record documents for WECC201102712 CIP-006-1 R3.1, included as Attachment b:

   1. URE1's Source Document;
   2. URE1's Revised Mitigation Plan designated as MIT-11-3807;
   3. URE1's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for WECC201102660 CIP-004-3 R3.2, included as Attachment c:

   1. URE2's Source Document;
   2. URE2's Mitigation Plan designated as MIT-11-3804;
   3. URE2's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for WECC201002653 CIP-006-1 R1.6, included as Attachment d:

   1. URE2's Source Document;
   2. URE2's Mitigation Plan designated as WECCMIT005170;
   3. URE2's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

e) Record documents for WECC201102651 CIP-006-1 R3, included as Attachment e:

   1. URE2's Source Document;

2. URE2's Mitigation Plan designated as MIT-11-3760;
3. URE2's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

f) Record documents for WECC201102798 CIP-006-1 R4, included as Attachment f:

1. URE2's Source Document;
2. URE2's Mitigation Plan designated as MIT-11-3860 ;
3. URE2's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for WECC201102671 CIP-007-1 R1, included as Attachment g:

1. URE3's Source Document;
2. URE3's Mitigation Plan designated as WECCMIT005630;
3. URE3's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

h) Record documents for WECC201002672 CIP-007-1 R3, included as Attachment h:

1. URE3's Source Document;
2. URE3's Mitigation Plan designated as MIT-10-3755;
3. URE3's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

i) Record documents for WECC201102799 CIP-007-2 R6, included as Attachment i:

1. URE3's Source Document;
2. URE3's Mitigation Plan designated as WECCMIT005631;
3. URE3's Certification of Mitigation Plan Completion ;
4. WECC's Verification of Mitigation Plan Completion;

j) Record documents for WECC201002673 CIP-007-1 R5.3.2, included as Attachment j:

1. URE3's Source Document;
2. URE3's Mitigation Plan designated as WECCMIT005391;
3. URE3's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[18]

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

[18] *See* 18 C.F.R § 39.7(d)(6).

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

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

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

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
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

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

Chris Luras*
Director 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
charles.berardesco@nerc.net

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments