PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

September 30, 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, 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 (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because the 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-002 R1; CIP-003 R6; CIP-004 R4; CIP-005 R1, R2, and R4; CIP-006 R1 and R6; CIP-007 R1, R3, and R8; CIP-008 R1; and CIP-009 R1, R2, R4, and R5. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC2013012117, WECC2012010602, WECC2012010757, WECC2012010596, WECC2012010597, WECC2012010748, WECC2012010758, WECC2012010735,

[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.

WECC2012010600, WECC2012010601, WECC2012010752, WECC2012010747, WECC2012010603, WECC2012010749, WECC2012010756, and WECC2012010755 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 entered into as of May 3, 2013, 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 (2013), 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	NOC-1940	WECC2013012117	CIP-002-3	R1	Medium	$150,000
			WECC2012010602	CIP-003-1	R6	Lower	
			WECC2012010757	CIP-004-1	R4	Lower	
			WECC2012010596	CIP-005-1	R1	Medium	
			WECC2012010597	CIP-005-1	R2	Medium	
			WECC2012010748	CIP-005-1	R4	Medium	
			WECC2012010758	CIP-006-1	R1	Medium	
			WECC2012010735	CIP-006-1	R6	Medium	
			WECC2012010600	CIP-007-1	R1	Medium	
			WECC2012010601	CIP-007-1	R3	Lower	

			WECC2012010752	CIP-007-1	R8	Medium	
			WECC2012010747	CIP-008-1	R1	Lower	
			WECC2012010603	CIP-009-1	R1	Medium/	
			WECC2012010749	CIP-009-1	R2	Lower	
			WECC2012010756	CIP-009-1	R4	Lower	
			WECC2012010755	CIP-009-1	R5	Lower	

CIP-002-3 R1

The purpose statement of Reliability Standard CIP-002-3 provides in pertinent part: "Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-3 R1 provides:

> R1. Critical Asset Identification Method — The Responsible Entity[4] shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
>
> > R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
> >
> > R1.2. The risk-based assessment shall consider the following assets:
> >
> > > R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.
> > >
> > > R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

[4] Within the text of the CIP Reliability Standards, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

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

[Footnote added.]

CIP-002-3 R1 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report to WECC stating it had a violation of CIP-002-3 R1. URE, in an attempt to be proactive and in anticipation of the effective date of April 1, 2014 for Version 4 of the CIP Standards, modified its risk-based assessment methodology to use the bright-line criteria proposed in CIP-002-4 R1 for its 2013 annual assessment and review of Critical Assets. WECC determined that URE failed to have a risk-based assessment methodology for identifying Critical Assets. Instead, URE used the bright-line criteria of Version 4 of the CIP Standards for its 2013 annual assessment and review of Critical Assets.

WECC determined the duration of the violation to be from when URE failed to document a risk-based methodology by revising its Critical Asset identification methodology that adopted the CIP-002-4 bright-line criteria for identifying its Critical Assets, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The updated methodology resulted in a single

generator facility no longer being classified as a Critical Asset. The generator had been identified earlier due to an overly-stringent criteria based on old documentation and guidance. Using a risk-based assessment methodology would still result in the generator not being classified as a Critical Asset. The declassified generator is 17% of URE's generation and is not classified as a blackstart facility.

CIP-003-1 R6

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

CIP-003-1 R6 provides:

> Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-003-1 R6.[5] As part of an internal review, URE discovered that it had failed to establish and document a process for configuration management by the time the Standard became mandatory and enforceable for URE. URE did not document a configuration management process or implement supporting configuration management activities to identify, control, and document all entity- or vendor-related changes to hardware and software components of Critical Cyber Assets (CCAs). Further, URE made configuration changes that did not follow procedures for its operating systems, patch levels, physical ports, and software enabled on all of its CCAs.

[5] WECC notified URE that WECC was initiating the Self-Certification process. Prior to the Self-Certification due date, URE submitted Self-Report addressing its noncompliance with CIP-003-1 R6; CIP-004-3 R4; CIP-005 R1, R2, and R4; CIP-006 R1 and R6; CIP-007 R1, R3, and R8; CIP-008-1 R1; and CIP-009-1 R1, R2, R4, and R5. Although URE self-reported these violations, because URE self-reported during the Self-Certification submission period, WECC considered the discovery method for these violations to be Self-Certification.

URE had a change management process in place using an automated solution to create and track master change requests. URE requires its support staff to create an activity ticket for all changes made to CCAs that are approved, and then sent to testing, where testing evidence must be gathered and approved before changes are made to production devices. Additionally, although URE was not formally maintaining documentation related to device configurations, some configuration information could be attained through the change tickets.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its baseline documentation.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed to establish a configuration management process, thereby potentially adding or modifying hardware and software changes that could expose the CCAs essential to the operation of the BPS to potential security vulnerabilities. As compensating measures, URE's CCAs are monitored and logged 24 hours a day, seven days a week, have antivirus and malware prevention tools, are located within a restrictive network, are backed up at least weekly, and all staff with access have cybersecurity training and personnel risk assessments (PRAs). Additionally, URE was maintaining documentation of ports and services enabled on the devices. Lastly, URE personnel stated URE had an automated change management solution in place that utilized a ticketing system for approvals and tracking, although it was not documented for the CCAs.

CIP-004-1 R4

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

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

CIP-004-1 R4 provides:

> R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

> R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
>
> R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
>
> R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

CIP-004-1 R4 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-004-1 R4. URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs. Specifically, URE did not conduct quarterly reviews of its lists of personnel who have access to CCAs, and did not revoke access to its CCAs within seven calendar days for four terminated personnel who no longer required such access.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its quarterly review of the access lists.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's 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. As compensating measures, the personnel in question were current on their PRAs and cybersecurity training before they left. The personnel were not terminated for cause. Badges were recovered and active directory access was removed for all personnel in scope. URE utilizes security guards and video recordings in its facilities 24 hours a day, seven days a week, and URE's host-based intrusion detection system would have generated an event if any of these employees tried to gain access.

CIP-005-1 R1 and R2

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

CIP-005-1 R1 and R2 provide:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
> >
> > R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
> >
> > R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

> R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R1 and R2 each have a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-005-1 R1 and R2. During the URE Cyber Vulnerability Assessment (CVA) for CIP-005, new access points to the Electronic Security Perimeter (ESP) were discovered. The access points were the result of devices with dual-homed network interface cards used for inter-control center communications protocol (ICCP) communications with neighboring transmission entities. URE failed to identify these access points in its ESP documentation. The devices in scope are ICCP servers which were originally identified as CCAs residing within an ESP; however, these devices were dual-homed with a second connection. Also as a result of the URE CVA, URE determined that the ESP firewall rules that control access to the ESP do not provide an adequate level of access control for the hosts by only filtering traffic based on the network address instead of specific addresses of machines. This assessment process led to the discovery of the dual-homed network interface cards self-reported in CIP-005 R1. The devices within the ESP in scope were used in support of the entity's control center.

WECC determined the duration of the CIP-005-1 R1 violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

WECC determined the duration of the CIP-005-1 R2 violation to be from the date the Standard became mandatory and enforceable, through when URE updated its firewall rule-set updates.

WECC determined that the violation of CIP-005-1 R1 posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Failure to document and implement mechanisms for control of electronic access to the ESP could allow unauthorized access to the ESP to go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets within the ESP. As compensating measures, the ICCP servers were identified and protected as CCAs. Specifically, URE personnel stated these devices were within a Physical Security Perimeter (PSP), with logging and monitoring configured for automated alerts upon unauthorized access. These devices reside in a network that was monitored by an intrusion detection system and the devices had antivirus and malware prevention tools. Additionally, the electronic access control and monitoring (EACM) devices in scope were located within a PSP where only vetted, trained, and authorized personnel had access, and all unauthorized access

was restricted and monitored through the use of card key controls. The devices, in addition to the network, also had antivirus and malware prevention tools installed.

WECC determined that the violation of CIP-005-1 R2 posed a minimal and not serious or substantial risk to the reliability of the BPS. Although firewall rules were too broad, the rules only allowed traffic from secured and trusted networks to other secured and trusted networks on a network-to- network basis. Additionally, URE stated all CCAs have implemented antivirus and malware prevention tools, and reside within a PSP that has six walls of protection with access-restrictive access points that only allow access to select individuals who are trained, vetted, and approved by designated personnel. Lastly, URE stated it actively logs all traffic both through and within its ESPs and any suspicious traffic is automatically alerted and sent to a control center or support staff to respond appropriately.

CIP-005-1 R4

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

CIP-005-1 R4 provides:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R4.1. A document identifying the vulnerability assessment process;
> >
> > R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
> >
> > 4.3. The discovery of all access points to the Electronic Security Perimeter;
> >
> > R4.4. A review of controls for default accounts, passwords, and network management community strings;

> R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

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

URE submitted a Self-Report to WECC stating it had a violation of CIP-005-1 R4. URE failed to perform an annual CVA of the electronic access points to its Energy Management System (EMS) ESPs. A penetration test was performed in 2010, but that test did not address CIP-005-1 R4. In 2011, there was no assessment completed. A full CVA was conducted by a third party in 2012 that fully addressed the Standard. The failure to perform an annual CVA resulted from a failure to assign responsibility to a URE manager responsible for compliance with the Reliability Standard and a lack of oversight by the existing URE compliance office during this time period.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to conduct a CVA could allow cyber vulnerabilities in URE's ESPs to go unchecked and undetected. Subsequently, such vulnerabilities could be exploited by malicious access, thereby providing an attack vector for launching cyber attacks against CCAs essential to the operation of BPS. As compensating measures, all ESPs implemented an intrusion detection system to detect malicious or suspicious network activity. Also, all Cyber Assets (including CCAs) implemented antivirus and malware prevention tools and were physically secured in a PSP with access limited to only individuals who were approved, vetted, and trained. All Cyber Assets (including CCAs) were monitored 24 hours a day, seven days a week by operators who would have detected any device outage. Additionally, the team responsible for maintenance and recovery of CCAs was on staff 24 hours a day, seven days a week. Lastly URE had documented operating procedures that could be used as a guide for operators to know whom to contact in case of a device outage.

CIP-006-1 R1

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

CIP-006-1 R1 provides:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
> >
> > R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
> >
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
> >
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005

Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

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

URE submitted a Self-Report to WECC stating it had a violation of CIP-006-1 R1. URE failed to afford the protective measures specified in Standards CIP-003 R6, CIP-007 R1, CIP-007 R3, CIP-007 R6, and CIP-009 R1 through R5 for six Cyber Assets used in the access control and monitoring of PSPs. The devices in scope are the entity's protection and control application server, protection and control database server, workstations, and controllers used in the access control and/or monitoring of the entity's PSPs. For CIP-003 R6, URE had no configuration management process for these devices; for CIP-007 R6, URE had no security status monitoring on the devices; for CIP-007 R1, URE had no test procedures or test environment; for CIP-007 R3, none of devices were included in the patch management process; and for CIP-009, URE had no documented recovery plans.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to ensure that Cyber Assets used in the access control and monitoring of the PSPs are afforded protective measures puts such assets at risk to be manipulated. For example, if ports and services required for normal operation of these access control and monitoring assets are not enabled, such ports and services could be utilized to gain unauthorized access to the PSP and go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets contained in the PSP. Such access may then be used to cause harm to CCAs essential to the operation of the BPS. The devices in scope were actively monitoring and logging all logical access and access attempts. They were also located in a secure network and located behind restrictive firewalls with limited access. The devices were also physically located in secure rooms with access limited by restrictive card keys access points, which only allow access to individuals with authorized access and approved PRAs and cybersecurity training. Lastly, the devices in scope implement antivirus and malware prevention tools.

CIP-006-1 R6

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 part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R6 provides:

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

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

URE submitted a Self-Report to WECC stating it had a violation of CIP-006-1 R6. URE failed to document its maintenance and testing program and failed to perform maintenance and testing on its physical security systems. URE has six devices used in the physical access control and monitoring of its PSPs.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to implement a maintenance and testing program to ensure that all physical security systems under CIP-006 were functioning properly could allow physical security systems to malfunction and allow unauthorized access to the PSP being monitored to go unnoticed and unchecked, thereby potentially allowing malicious physical access to Cyber Assets within the PSP. URE's CCAs and devices used in the physical access control and monitoring have electronic monitoring and logging 24 hours a day, seven days a week, have antivirus and malware

prevention tools, are located within a restrictive network, and are backed up at least weekly. All staff with access to the CCAs and devices are trained and vetted with current PRAs and CIP cybersecurity training. Additionally URE was maintaining documentation of ports and services enabled on the devices.

CIP-007-1 R1

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

CIP-007-1 R1 provides:

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

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

URE submitted a Self-Report to WECC stating it had a violation of CIP-007-1 R1. Through an internal assessment, URE discovered that it did not document formal test procedures and archive test results of significant changes for its non-Windows Cyber Assets. URE failed to create, implement, and maintain cybersecurity test procedures and failed to ensure significant changes did not adversely affect the production environment. Specifically, URE stated that since its initial compliance date, for all non-

Windows devices, it had not created or implemented procedures to ensure changes to existing Cyber Assets within the ESP that did not adversely affect existing cybersecurity controls. The devices in scope are switches, servers, and encryptors that perform the functions of the EMS and distributed control systems (DCS) environments.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to create cybersecurity test procedures for the Cyber Assets within an ESP could allow untested and potentially malicious changes, such as patch, service pack, vendor release, application or database updates, to be released in the production systems. In addition, lack of cybersecurity test procedures could fail to detect and prevent potentially harmful modifications to existing security controls for CCAs. Such issues could introduce cybersecurity vulnerabilities into the CCAs essential to the operation of the BPS from the functions of the EMS and DCS environments. As compensating measures, URE implemented active monitoring and logging, and antivirus and malware prevention tools, and all devices resided within an ESP and PSP. URE also implemented an automated solution called "secret server" that monitors all administrator accounts and passwords. Lastly, all individuals with access to the devices had current PRAs and cybersecurity training, and URE conducted annual reviews of accounts and ports/services on all devices.

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.

URE submitted a Self-Report to WECC stating it had a violation of CIP-007-1 R3. URE implemented a patch management program for its Windows Cyber Assets within two of its ESPs. Security patches and upgrades for those Windows devices have been evaluated within 30 calendar days of their availability and scheduled for implementation. However, URE failed to implement a patch management program that encompassed all non-Windows devices within these ESPs. Within the URE DCS environments, patch management is contracted to the maintenance and support vendors who perform annual patching of those systems during annual maintenance windows. URE has no evidence that the reviews of security patches or upgrades were reviewed within 30 calendar days of their availability. URE failed to document compensating measures for those non-Windows security patches and upgrades that were not evaluated within 30 calendar days of their availability.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, a 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. This increased risk may allow for unauthorized internal and or external access, which could allow for successful cyber attacks against CCAs essential to operation of the BPS. As compensating measures, all devices implemented active monitoring and logging andantivirus and malware prevention tools, and resided within an ESP and PSP. URE also implemented an automated solution called "secret server" that monitors all accounts and passwords. Lastly, all individuals with access to the devices had current PRAs and training, and URE conducted annual reviews of accounts and ports/services on all devices.

CIP-007-1 R8

The purpose statement of Reliability Standard CIP-007-1 provides:

> 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 other (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 R8 provides:

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

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

URE submitted a Self-Report to WECC stating it had a violation of CIP-007-1 R8. URE failed to perform an annual CVA of all assets within its EMS ESPs. From 2010 through 2011, URE did not complete a formal assessment. A full CVA was conducted by a third party in 2012 that fully addressed the requirements of the Standard. For URE's generation assets at one of its facilities, a full CVA that met the requirements of the Standard was conducted in 2010 by a third party. In 2011, there was no assessment completed. A full CVA that fully addressed the requirements of the Standard was conducted by a third-party in 2012.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to conduct a CVA of all Cyber Assets could allow cyber vulnerabilities in such assets to go unchecked and undetected. Subsequently, such vulnerabilities could be exploited by malicious access, thereby providing an attack vector for launching

cyber attacks against CCAs essential to the operation of BPS. As compensating measures, all ESPs implemented an intrusion detection system to detect malicious or suspicious network activity. Also, all Cyber Assets (including CCAs) implemented antivirus and malware prevention tools, and were physically secured in a PSP with access limited to only individuals who were approved, vetted, and trained. All Cyber Assets (including CCAs) were monitored 24 hours a day, seven days a week by operators who would have detected any device outage. Additionally, the team responsible for maintenance and recovery of CCAs was on staff 24 hours a day, seven days a week. Lastly, URE had documented operating procedures that could be used as a guide for operators, specifying whom to contact in case of a device outage.

CIP-008-1 R1

The purpose statement of Reliability Standard CIP-008-1 provides: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-008-1 R1 provides:

> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:
>
> > R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
> >
> > R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
> >
> > R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.
> >
> > R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.

> R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
>
> R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-008-1 R1 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-008-1 R1. URE failed to document a Cyber Security Incident response plan (CSIRP) of sufficient detail that contained specific roles and responsibilities of the response team. While a plan existed, specific actions and participants were not defined to respond to each type of event that could be classified as a Cyber Security Incident. In addition, URE failed to test its CSIRP on an annual basis.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable through when URE updated its CSIRP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it lacked sufficient detail, URE did have a CSIRP in place. URE's CCAs have protections in place at all times apart from a CSIRP, the CCAs have electronic monitoring and logging 24 hours a day, seven days a week, have antivirus and malware prevention tools, are located within a restrictive network, are backed up at least weekly, and all staff with access are trained and vetted as per CIP-004. Additionally, URE was maintaining documentation of ports and services enabled on the devices.

CIP-009-1 R1, R2, R4, and R5

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

CIP-009-1 provides in pertinent part:

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

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

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

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

*****

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

CIP-009-1 R1 has a "Medium" VRF and a "Severe" VSL. CIP-009-1 R2, R4, and R5 each have a "Lower" VRF and "Severe" VSL.

URE submitted a Self-Report to WECC stating it had a violation of CIP-009-1 R1. URE submitted a Self-Report to WECC stating it had a violation of CIP-009-1 R2. URE submitted a Self-Report to WECC stating it had a violation of CIP-009-1 R4 and R5. As part of an internal assessment conducted by URE compliance personnel, URE discovered that it failed to create and annually review its recovery plan for CCAs.

URE had a "shell" of a high-level recovery plan for its CCAs that was not specific to all CCAs, and did not specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan, or define the roles and responsibilities of responders (R1); URE did not annually exercise its plan, or use it in an actual incident (R2); URE's plan did not include processes and procedures for the backup and recovery of backup and storage of information required to successfully restore CCAs; it had no formal procedures for ensuring all CCAs were backed up, and URE was not ensuring other forms of backup were in place, such as spare electronic components and

equipment (R4); and URE failed to ensure information essential to recovery that is stored on backup media was tested at least annually in the calendar year to ensure that the information is available (R5).

WECC determined the duration of the violations to be from the date the Standard became mandatory and enforceable through when URE completed its Mitigation Plans.

WECC determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically for R1, failure to ensure that recovery plans are in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices could render CCAs essential to operation of BPS as irrecoverable and non-operational in the event of a cybersecurity incident, thereby negatively impacting the reliability of the BPS. For R2, failure to exercise the recovery plan at least annually could prevent the entity from determining the proficiency of the plans and could lead to recovery plans that are ineffective which could render CCAs essential to the operation of BPS as irrecoverable and thereby non-operational in the event of a cybersecurity incident, thus negatively impacting the reliability of the BPS. For R4, failure to ensure that the recovery plan include processes and procedures for the backup and storage of information required to successfully restore CCAs could render CCAs essential to operation of BPS as irrecoverable and thereby nonoperational in the event of a cybersecurity incident. Finally, for R5, failure to annually test information essential to recovery that is stored on backup media could lead to recovery plans that are ineffective which could render CCAs essential to operation of the BPS as irrecoverable and thereby non-operational in the event of a cybersecurity incident, thus negatively impacting the BPS.

As compensating measures, URE's CCAs implemented antivirus and malware prevention tools, were in a network with restrictive boundary devices, were physically secured in a PSP with access limited to only individuals who were approved, vetted, and had received cybersecurity training. All CCAs were monitored by operators 24 hours a day, seven days a week who would have detected any device outage. Additionally, the team responsible for maintenance and recovery of CCAs was on staff 24 hours a day, seven days a week. Lastly, URE had documented operating procedures that could be used as a guide for operators on the appropriate persons to contact in case of a device outage.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE's previous violations were not considered aggravating factors in the penalty determination. URE's previous violations were of different requirements than the instant violations. Moreover,

WECC determined there was nothing in the record to suggest that broader corporate issues were implicated;

2. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE self-reported the CIP-002-3 R1 violation;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;
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 of CIP-002-3 R1, CIP-005-1 R2, and CIP-008-1 R1 posed a minimal risk to the reliability of the BPS and that the remaining violations posed a moderate risk to the reliability of the BPS. None of the violations posed a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. 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 thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-002-3 R1

URE's Mitigation Plan to address its violation of CIP-002-3 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008993 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Re-write its RBAM to utilize the criteria defined in the *NERC Security Guideline for the Electric Sector: Identifying Critical Assets*;
2. Obtain senior manager review and approval of the modified RBAM;
3. Perform the assessment of URE assets using the modified RBAM with URE subject matter experts;

[6] *See* 18 C.F.R § 39.7(d)(7).

4. Collect supporting evidence for the responses to the RBAM criteria applied to each asset;
5. Review the assessment results and supporting evidence with the senior manager;
6. Obtain senior manager approval of the Critical Asset List;
7. Submit the completed mitigation plan and all supporting evidence to WECC; and
8. Collect supporting evidence to justify the criteria and responses.

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

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

CIP-003-1 R6

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008117 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop a short term manual plan;
2. Document a compliance procedure for change management and configuration management;
3. Develop a long-term solution (Tripwire) for compliance;
4. Establish manual temporary measures to capture Windows, Cisco, and "Other" device configurations;
5. Document an operational procedure for capturing device configurations for all device types (Windows, Cisco, other);
6. Implement use of the new operational procedure for configuration management into URE's change management processes; and
7. Ensure the use of the compliance checklist as part of URE's change management process includes capturing configurations as part of any CCA addition or modification.

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

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

CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007892 and was submitted as non-public information to FERCin accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop an access management program that incorporates the granting and tracking of physical access to PSPs, logical access to CCAs, and access to protected information;
2. Develop a database to track and report on all employees and contractors with physical access to PSPs, logical access to CCAs, and access to protected information;
3. Assign responsibility for access administration to appropriate resources;
4. Develop email distribution lists for notification of access approvals, removals, quarterly reviews, and terminations;
5. Develop report formats for quarterly reviews that demonstrate all access granted for each employee/contractor;
6. Perform training for all access administrators; and
7. Set calendar triggers/reminders for quarterly and annual reviews in GenSuite.

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

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

CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007806 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Open change management request (CMR);
2. Obtain CMR approvals;
3. Remove dual-home network interface cards on the two devices;
4. Modify firewall rule-set to allow ICCP traffic from the two hosts;
5. Update ESP diagrams and all associated documentation;
6. Capture new configurations for each device;
7. Close CMR;
8. Develop a new checklist for use by the compliance office as part of the CMR closure process; and
9. Modify CMR closure process for new checklist.

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

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

CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007805 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Open CMR;
2. Hire and complete orientation of a new network resource;
3. Develop firewall rule testing/review procedure;
4. Draft modified rulebase;
5. Audit Objects Group;
    a. Define/identify component owners;
    b. Provide firewall rules and review with component owners;

c. Follow up with each component owner;

d. Finalize initial object groups;

6. Firewall test for Distributed Component Object Model (DCOM) traffic;
    a. Add front ends to test environment;
    b. Identify DCOM traffic that is required between devices;
    c. Refine DCOM Rules;
7. Implement new firewall rules;
8. Complete eight Iterations;
    a. Perform firewall review procedure;
    b. Remove/Modify several rules from rule base;
    c. Analyze/monitor traffic;
    d. Refine rules and groups as needed;
9. Update all appropriate documentation;
10. Close CMR;
11. Implement quarterly reviews of firewall rules;
12. Develop a new checklist for use by the compliance office as part of the CMR closure process; and
13. Modify CMR Closure Process for new checklist.

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

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

CIP-005-1 R4

URE's revised Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007978 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Determine the project resource strategy - in-house versus external vendor;
2. Engage CVA vendors to perform the assessment;
3. Develop a CVA procedure;
4. Ensure all requirements were addressed in the vendor assessment process;
5. Use a mix of active and passive approaches to the CVA;
6. Review the vendor CVA report and determine appropriate actions;
7. Prepare a remediation plan;
8. Assign resources to address remediation actions and accepted recommendations;
9. Follow change management and configuration management processes to address remediation actions and accepted recommendations;
10. Track remediation plan until all items are closed; and
11. Create a calendar event to trigger the annual CVA project.

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

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

CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007893 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement PAC monitoring systems (PACMS) configuration management;
2. Modify change management process;
3. Complete PACMS recovery plan and exercises;
4. Complete PACMS test procedures and test environment;
5. Complete PACMS patch management; and

6. Implement PACMS log reviews.

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

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

CIP-006-1 R6

URE's Mitigation Plan to address its violation of CIP-006-1 R6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008277 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop a Physical Security Maintenance and Testing Program document;
2. Develop an inventory of all devices that comprise the physical security systems;
3. Work with the physical security integrator (vendor) to determine the basis and frequency of testing/maintenance for each physical security device;
4. Establish a contract with the physical security integrator to perform the testing and maintenance;
5. Perform the baseline testing and maintenance for each physical security device;
6. Enhance the security operations center procedures to include physical security outage records management; and
7. Create a calendar event to trigger the testing and maintenance activities for the physical security systems.

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

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

CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated

as WECCMIT007859 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Perform an analysis of the production environments and identify comparable Cyber Assets required in the test environment;
2. Procure additional Cyber Assets required for the test environment;
3. Configure and install new Cyber Assets in the test environment;
4. Ensure that new Cyber Assets in the test environment reflect the same operating system versions, firmware versions, and all other software reflect the same version levels as production;
5. Update test environment documentation;
6. Confirm platforms that require new or modified test procedures;
7. Develop test procedures based upon the enhanced test environment and ensure that test procedures address all security controls for the device type;
8. Refine test procedures as a result of applying security patches to the new Cyber Assets in the test environment; and
9. Update all applicable policy documentation associated with testing.

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

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

CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. URE submitted a Mitigation Plan extension request with a revised completion date. WECC accepted URE's extension request. The Mitigation Plan for this violation is designated as WECCMIT007860 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Enhance URE patch management procedures and tracking process to include Cisco and other device patches;
2. For Windows patches not previously evaluated:
    a. Identify, evaluate, and test any additional/new Windows patches in test environment.
    b. Revise implementation plan to group patches by Windows Cyber Asset type.
    c. Open CMR for Windows.
    d. Implement Windows patches in Production - Stage 1 Workstations;
    e. Implement Windows patches in Production - Stage 2 - Servers and DCs;
    f. Implement Windows patches in Production - Stage 3 – ICCP;
    g. Implement Windows patches in Production - Stage 4 - CORE Secondary; and
    h. Implement Windows patches in Production - Stage 5 - CORE Primary.
    i. Close CMR.
3. For Cisco patches:
    a. Engage new Network Team resource;
    b. Identify, evaluate, and test Cisco patches in test environment;
    c. Develop implementation plan for Cisco devices;
    d. Open CMR for Cisco devices;
    e. Implement Cisco patches in Production; and
    f. Close CMR.
4. Other device patches:
    a. Procure additional Cyber Assets required for the test environment;
    b. Configure and install new Cyber Assets in the test environment;
    c. Identify missing patches;
    d. Develop test procedures based upon the enhance test environment and ensure that test procedures address all security controls for the device type;
    e. Refine test procedures and test Implementation of patches in the test environment;

f. Plan the production implementation of all patches;

g. Open CMR;

h. Implement all patches in production; and

i. Close CMR.

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

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

CIP-007-1 R8

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007979 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Determine the project resource strategy - in-house versus external vendor;
2. Engage CVA vendors to perform the assessment;
3. Develop a CVA procedure;
4. Ensure all requirements were addressed in the vendor assessment process;
5. Use a mix of active and passive approaches to the CVA;
6. Review vendor CVA report and determine appropriate actions;
7. Assign resources to address remediation actions and accepted recommendations;
8. Follow change management and configuration management processes to address remediation actions and accepted recommendations;
9. Track remediation plan until all Items are closed; and
10. Create a calendar event to trigger the annual CVA project.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan.
Aafter reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-008-1 R1

URE's Mitigation Plan to address its violation of CIP-008-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008020 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review current CSIRP to identify missing components;
2. Develop action plans for each security event scenario that could escalate into a cybersecurity incident;
3. Identify and assign responsibilities for each cybersecurity incident scenario, including reporting to ES ISAC;
4. Revise and publish updated CSIRP;
5. Conduct an annual review of CSIRP;
6. Conduct an annual test of CSIRP;
7. Update CSIRP with any identified changes from the annual review/test; and
8. Set up a GenSuite calendar event to ensure the annual review and test of the URE CSIRP.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its Mitigation Plan.
After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-009-1 R1, R2, R4, and R5

URE's Mitigation Plans to address its violations of CIP-009-1 R1, R2, R4, and R5 were submitted to WECC. The Mitigation Plans were accepted by WECC and approved by NERC. The Mitigation Plans for these violations are designated as WECCMIT007934 (R1), WECCMIT007935 (R2), WECCMIT007936 (R4), and WECCMIT007937 (R5), and were submitted as non-public information to FERCin accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Ensure that recovery of all CCAs, PACMS, and electronic access control or monitoring system devices are accounted for in the recovery plan;

2. Verify that all Cyber Assets included in the recovery plan are included in the enterprise backup strategy;
3. Publish revised recovery plan;
4. Perform an annual review of the recovery plan;
5. Perform tabletop exercise;
6. Perform testing of backup media; and
7. Set calendar triggers/reminders for annual review of the recovery plan in GenSuite.

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

After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plans were completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 10, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifty thousand dollar ($150,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE's previous violations did not constitute prior violations and were not considered aggravating factors in the penalty determination. URE's previous violations were of requirements that are not same or similar to the instant violations. Moreover, WECC

[7] *See* 18 C.F.R. § 39.7(d)(4).
[8] *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).

determined there was nothing in the record to suggest that broader corporate issues were implicated;

2. URE had a compliance program at the time of the violation which WECC considered a mitigating facto;
3. URE self-reported the CIP-002-3 R1 violation;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

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, included as Attachment a;

b) Self-Certification for the violations of CIP-003-1 R6; CIP-004-3 R4; CIP-005 R1, R2, and R4; CIP-006 R1 and R6; CIP-007 R1, R3, and R8; CIP-008-1 R1; and CIP-009-1 R1, R2, R4, and R5, included as Attachment b;

c) Record documents for the violation of CIP-002-3 R1, included as Attachment c:

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT008993;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-003-1 R6, included as Attachment d:

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT008117;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

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

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT007892;
   3. WECC's Verification of Mitigation Plan Completion;

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

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT007806;
   3. URE's Certification of Mitigation Plan Completion;

4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-005-1 R2, included as Attachment g:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007806;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-005-1 R4, included as Attachment h:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007978;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-006-1 R1, included as Attachment i:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007893 submitted;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-006-1 R6, included as Attachment j:

1. URE's Mitigation Plan designated as WECCMIT008277;
2. URE's Certification of Mitigation Plan Completion;
3. WECC's Verification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-007-1 R1, included as Attachment k:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007859;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-007-1 R3, included as Attachment l:

1. URE's Source Document;

2. URE's Mitigation Plan designated as WECCMIT007860;
3. WECC's Notice of Mitigation Plan Extension Request Acceptance;
4. URE's Certification of Mitigation Plan Completion;
5. WECC's Verification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-007-1 R8, included as Attachment m:

1. URE's Source Document;
2. URE's Revised Mitigation Plan designated as WECCMIT007979;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

n) Record documents for the violation of CIP-008-1 R1, included as Attachment n:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT008020;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-009-1 R1, included as Attachment o:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007934;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

p) Record documents for the violation of CIP-009-3 R2, included as Attachment p:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007935;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-009-3 R4, included as Attachment q:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007936;

3. WECC's Verification of Mitigation Plan Completion;

r) Record documents for the violation of CIP-009-3 R5, included as Attachment r:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT007937; and
3. WECC's Verification of Mitigation Plan Completion.

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

Sonia C. Mendonça
Assistant General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline*
North American Electric Reliability Corporation
Senior Counsel and Associate Director, Enforcement Processing
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments