NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 28, 2016

VIA ELECTRONIC FILING

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. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2] 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)).[3]

NERC is filing this Notice of Penalty 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 of CIP-002, CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007.

---

[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 (2015). *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] 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.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty 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, by and between WECC and URE. The details of the findings 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 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC201002262	CIP-002-1	R1; R1.2; R1.2.2; R1.2.4	Medium/ Severe	SC	No Penalty
WECC201002354	CIP-002-1	R3; R3.1	High/ Severe	CA	
WECC201002355	CIP-003-1	R1; R1.1; R1.2; R1.3	Medium/ Severe	SR	
WECC201002356	CIP-003-2	R4.3	Medium/ Severe	SR	
WECC2013011670	CIP-003-3	R5	Lower/ Severe	SR	
WECC200801173	CIP-004-1	R2	Lower/ Severe	SR	
WECC200801174	CIP-004-1	R3	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC2014014185	CIP-004-3a	R3	Medium/ Severe	SR	No Penalty
WECC201002280	CIP-004-1	R3; R3.2	Medium/ High	SR	
WECC200801175	CIP-004-1	R4	Lower/ Lower	SR	
WECC201002381	CIP-005-1	R1	Medium/ Severe	SR	
WECC201102851	CIP-005-1	R1; R1.4	Medium/ Severe	SR	
WECC200901633	CIP-005-1	R1; R1.5	Lower/ Lower	SR	
WECC201002382	CIP-005-1	R2	Medium/ Moderate	SR	
WECC2013013087	CIP-005-3	R3; R3.2	Medium/ Severe	CA	
WECC201002269	CIP-006-1	R1; R1.6	Medium/ Severe	SR	
WECC200901632	CIP-006-1	R1; R1.8	Lower/ Lower	SR	
WECC201002273	CIP-006-1	R4	Lower/ Moderate	SR	
WECC2015014618	CIP-006-3c	R5	Medium/ Severe	SR	
WECC200801176	CIP-007-1	R1	Medium/ Severe	SR	
WECC201002260	CIP-007-1	R1; R1.1	Medium/ Severe	SR	
WECC2015014628	CIP-007-1	R2	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC200902261	CIP-007-1	R3; R3.1	Lower/ Severe	SR	No Penalty
WECC2015014629	CIP-007-1	R5	Medium/ Severe	SR	
WECC201002412	CIP-007-1	R5; R5.2.2	Lower/ Severe	SR	
WECC201002279	CIP-007-1	R6; R6.4; R6.5	Medium/ Severe	SR	

WECC201002262 CIP-002-1 R1; R1.2; R1.2.2; R1.2.4 - OVERVIEW

WECC determined that URE did not consider transmission facilities at certain facilities in its Risk-Based Assessment Methodology (RBAM), in violation of CIP-002 R1. Specifically, WECC determined that URE failed to consider: 1) all assets that support reliable Bulk Electric System (BES) operations at two locations, in violation of CIP-002-1 R1.2; 2) transmission substation assets at two locations, in violation of CIP-002-1 R1.2.2; and 3) transmission assets identified as critical to system restoration at six locations, in violation of CIP-002-1 R1.2.4.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). This violation created the opportunity for misidentified or unidentified Critical Assets that pose risks associated with unidentified Critical Cyber Assets (CCAs). In this case, URE failed to consider all transmission substations and substations that support the reliable operation of the BPS or that are critical to system restoration in its RBAM. The risks posed by URE's noncompliance are, to some extent, lessened in that URE did document and implement an RBAM that resulted in identification of a number of Critical Assets including other substations and control centers.

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.

URE submitted its Mitigation Plan designated WECCMIT004842-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete development and full documentation of its RBAM;
2. apply the RBAM to test its validity on a subset of URE-owned assets;

3. submit its RBAM to WECC for review;
4. discuss WECC feedback on URE's RBAM;
5. modify its RBAM, if necessary, as a result of feedback from WECC;
6. complete list of all assets for use in applying RBAM;
7. apply its RBAM to all assets; and
8. develop a list of Critical Assets for URE's area.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002354 CIP-002-1 R3; R3.1 - OVERVIEW

WECC determined that URE did not identify CCAs associated with Critical Assets located at multiple locations including substations and control centers.

WECC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Compromise of the unprotected devices could cause significant disruption of normal operations within URE's area, including the risk of substantial loss of load. In this case, URE failed to identify relays and the Control Center Cyber Assets, described herein, as CCAs. The scope of the violation includes CCAs at both URE's Control Centers and critical substations. Without proper identification, these CCAs were vulnerable to cyber security attacks.

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.

URE submitted its Mitigation Plan designated WECCMIT004840-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document URE consolidated (field and control center) CCA identification methodology;
2. ensure CIP protections through obtaining attestations from CCA asset owners and/or enter into some type of agreement;
3. modify CCA identification methodology to reflect any RBAM changes that occurred as a result of feedback from WECC on URE's RBAM;
4. apply CCA identification methodology and develop list of CCAs for URE's control centers;

5. complete analysis of approaches to ensure identification and protection of CCAs at Critical Asset sites;
6. notify all asset owners of non-URE owned Critical Assets and request a list of associated Cyber Assets;
7. notify WECC of any non-URE Critical Asset owners that did not provided URE with its list of Cyber Assets, as requested above;
8. apply CCA identification methodology to develop list of CCAs for URE-owned field assets and for non-URE-owned Critical Assets;
9. notify owners of non-URE-owned CCAs of URE's CCA determination and of the need for delegation agreements;
10. complete delegation agreements; and
11. notify WECC of any non-URE Critical Asset owners for which URE has identified CCAs with which URE cannot reach agreement.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002355 CIP-003-1 R1; R1.1; R1.2; R1.3 - OVERVIEW

WECC determined that for one year, URE's cyber security policy failed to address over 20 CIP requirements, in violation of CIP-003-1 R1.1. WECC also determined that URE failed to make its cyber security policy available to all personnel with physical access to CCAs at one facility, in violation of R1.2. Finally, WECC determined that URE's CIP senior manager failed to annually review and approve one chapter in URE's cyber security policy, as required under R1.3.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Given that the one facility houses URE's Control Center and is a Critical Asset with CCAs identified by URE, noncompliance described herein potentially threatens the security of URE CCAs essential to URE Control Center operability. The risks, however, are somewhat diminished in that the cyber security policy did address 18 of the requirements for which URE was required to reach compliance. Further, the cyber security policy was made available to personnel with access to its intranet site and was posted at all but two facility entrances.

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.

URE submitted its Mitigation Plan designated WECCMIT004694 to address the referenced violations. URE's Mitigation Plan required URE to:

1. ensure its CIP senior manager reviewed, approved, and issued cyber security policies on specific CIP Standards;
2. ensure its CIP senior manager reviewed and approved the grid operations information system security program manual (ISSP Manual);
3. develop a process for issuing and tracking hard copy versions of the ISSP Manual;
4. place hard-copy versions of the ISSP Manual at various points in the control centers; and
5. create awareness posters indicating location of the ISSP Manual, and send e-mail to all personnel with physical access to the control centers.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002356 CIP-003-2 R4.3 - OVERVIEW

WECC determined that although URE conducted an "annual review" of its CCA information protection program (IP Program) pursuant to CIP-003-2 R4, URE failed to assess adherence to its IP Program following implementation, in violation of CIP-003-2 R4.3

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to protect information associated with CCAs may render Cyber Assets vulnerable to misuse or malicious attack. The risks posed by URE's noncompliance are, to some extent, lessened in that URE demonstrated that it documented and implemented an IP Program.

WECC determined the duration of the violation to be from the date URE was required to assess adherence to its program, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT093456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review its ISSP Manual to ensure compliance;
2. review and revise its ISSP Manual to include process to inventory all documents requiring CIP protections;
3. complete an annual review of document inventory;
4. develop a project plan for increased scope of the potential violation;

5. complete its project plan for this Mitigation Plan;
6. develop and prepare appropriate material for identifying and protecting information that requires protection;
7. develop an information protection assessment program;
8. revise, rename, and republish ISSP Manual and related supporting documents;
9. provide CIP subject matter expert (SME) training on procedures and requirements;
10. distribute attestations and instructions to managers responsible for reviewing their organizations' CCA information;
11. provide annual entity-wide training on URE's IP Program; and
12. complete the annual assessment of adherence to the IP Program for CCA information and prepare a written report on the results of the annual assessment.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2013011670 CIP-003-3 R5 - OVERVIEW

WECC determined that URE placed two documents on its SharePoint site without implementing access management controls. Any individual with access to the SharePoint site would have had access to the documents irrespective of any authorization. WECC also determined that URE disclosed one of the documents to an external vendor that did not have authorization to view protected CCA information. Finally, URE posted videos on social media containing footage that included CCAs or facility information.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The unprotected information disclosed by URE was associated with CCAs associated with URE control centers. URE afforded these devices a number of protections. URE physically secured the devices in scope of the violation from unauthorized access within Physical Security Perimeters (PSPs). Physical access to the devices was restricted to individuals who completed personnel risk assessments (PRAs) and cyber security training. URE onsite security personnel logged and monitored physical access and physical access attempts—unauthorized access attempts would have triggered alarming.

URE also electronically secured the CCAs within an Electronic Security Perimeter (ESP). Again, individuals with electronic access to the devices completed PRAs and cyber security training. Electronic

access was restricted to individuals who required such access. Electronic access and electronic access attempts were logged and monitored. Cyber security events would have triggered alarming.

WECC determined the duration of the violation to be from the date URE posted on social media, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT008826 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise and redistribute the memorandum that designated personnel responsible for authorizing logical or physical access to protected information (as required by CIP-003-3 R5.1). This would ensure that (a) the list of personnel responsible for authorizing logical or physical access is current and (b) that the memorandum references the marking, safeguarding, and sharing of documents that contain CCA-protected information;
2. provide additional training for personnel responsible for authorizing logical or physical access to CCA-protected information and their managers regarding their responsibilities;
3. establish procedures that ensure that personnel do not allow videos and/or pictures to be taken of Control Center facilities without proper authorization; and
4. establish an agreed-upon procedure between URE's information security group and public affairs group concerning the sharing and posting of any document, video, or images that contain NERC CIP Critical Information.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801173 CIP-004-1 R2 - OVERVIEW

WECC determined that URE did not ensure it trained all personnel having access to CCAs in a special program for personnel with access to CCAs by the compliance date.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's personnel have participated in the annual cyber security and security refresher training. The relevant workstations with access to the Control Center network (CCN) are located within secure URE facilities. Cyber access and unescorted physical access to cyber assets that enable control of transmission or electric power generation is limited to personnel whose jobs require that they have access to the assets and who have completed the training required under CIP-004-1 R2.2. The CCN was a closed network. The firewall rules are defined based on the policy that no connections initiated external to the ESP of the CCN are permitted inbound through the ESP firewall.

Network intrusion detection devices are installed on all network segments internal and external to the ESP of the CCN. Personnel with administrative cyber access rights to CCAs are identified, and access is limited to maintenance personnel. Access to control center CCAs is limited to entity employees and contractor employees. Physical access is controlled through combinations of identification cards, proximity card key access control systems, closed circuit cameras, and/or security personnel. CCAs are monitored continuously by control center maintenance personnel to ensure they are functioning properly.

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.

URE submitted its Mitigation Plan designated MIT-08-1205 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training on control center CCAs;
2. identify changes to the ESP, PSP, and CCA security controls to further limit access to CCAs;
3. implement changes identified above;
4. identify and train any remaining personnel with cyber and unescorted physical access to control center CCAs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801174 CIP-004-1 R3 - OVERVIEW

WECC determined that URE did not complete PRAs for all contractor employees by the compliance deadline.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All URE employees have had the required background investigation, although not all have been reassessed in the last seven years. URE's process has required identity verification of all new URE and contract employees for over ten years. Therefore, the risk of current URE or contract employees never having had a background investigation is low.

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.

URE submitted its Mitigation Plan designated WECCMIT081206 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014185 CIP-004-3a R3 - OVERVIEW

WECC determined that URE did not update one PRA that expired after seven years for a contract employee in good standing.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented preventative controls, such as multiple layers of user names and passwords with varying levels of clearance, which the person in scope did not have, to get access to CCAs. URE also uses two-factor authentication, requiring a randomly generated number in addition to a four-digit PIN, neither of which the person in scope had. URE implemented detective controls, such as logs of all physical access attempts, both successful and unsuccessful, which would allow the entity to know if/when the person in scope entered a substation. URE monitors all trip and close operations, which generate alarms to alert personnel of issues. Personnel also receive alarms for unauthorized breaker operations or relay failures. As a corrective control, URE personnel can remotely operate relays and breakers to maintain system stability. URE also has procedures to respond to emergencies. As compensating controls, URE logically separates its substations, not allowing anyone with access to one substation to access other substations, meaning that a malicious person would have to go to each substation to load a virus, which could give the entity more time to detect any issues.

WECC determined the duration of the violation to be from the date URE should have updated the PRA, through when URE completed the PRA.

URE submitted its Mitigation Plan designated WECCMIT010933 to address the referenced violations. URE's Mitigation Plan required URE to:

1. make minor revisions of the PRA verification checklist to include a reviewer verification field; and
2. make modifications to the standard operating procedure (SOP) to include verbiage that instructs staff not to approve initial PRA verification requests when the PRA is within six months of expiration. Instead the staff member whose PRA is expiring will be contacted and notified that they must complete the PRA renewal process before approval is granted.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002280 CIP-004-1 R3; R3.2 - OVERVIEW

WECC determined that URE did not update each PRA at least every seven years after the initial PRA. In a second instance, WECC determined that URE failed to conduct a PRA within 30 days of personnel receiving access to CCAs. Finally, URE identified three additional instances wherein it granted access to CCAs to personnel without completing a recurring PRA every seven years.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All employees did complete and pass initial identity verification. Further, all employees underwent a criminal background check at the time of hiring.

WECC determined the duration of the violation to be from 30 days after URE granted access to an employee without the employee having a valid PRA, through when URE completed all recurring PRAs.

URE submitted its Mitigation Plan designated MIT-09-3456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop e-mail templates to notify organizations which grant or revoke authorized unescorted physical or cyber access;
2. complete a review of hard-copy documentation for all employees having authorized cyber or authorized unescorted physical access to CCAs;
3. document procedures for a quarterly random sample review of hard-copy documentation of seven-year criminal check and personal identity verification;
4. revoke cyber and/or physical access to CCAs for employees without a timely criminal check and personal identity verification;
5. complete seven-year criminal checks and personally identify verification for any employees whose access was revoked above;

6. review all SOPs regarding criminal checks and personal identity verifications to ensure they provide adequate quality assurance and quality control measures.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801175 CIP-004-1 R4 - OVERVIEW

WECC determined that URE did not fully document the specific electronic or unescorted physical access rights of all URE personnel with access to CCAs by the compliance date. The ESP of the Control Center network (CCN) expanded beyond the PSP of the Control Center.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All workstations with CCN access are located within secure URE facilities. URE requires all employees complete mandatory Annual Cyber Security and Security Refresher Training on URE policies pertaining to the protection of all URE sensitive information and information systems including CCAs. Cyber access and unescorted physical access to critical cyber assets that enable control of transmission or electric power generation is limited to Control Center users and support staff. The CCN is a closed network. The firewall rules are defined based on the policy that no connections initiated external to the ESP of the CCN are permitted inbound through the ESP firewall. Network intrusion detection devices are installed on all network segments internal and external to the ESP of the CCN. Personnel with administrative cyber access rights to CCAs are identified. Access to Control Center CCAs is limited to URE employees and contract employees. Physical access is controlled through identification cards, proximity card key access control systems, closed circuit cameras, and security personnel. Control center maintenance personnel continuously monitor the proper functioning of CCAs.

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.

URE submitted its Mitigation Plan designated MIT-08-1207 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training on control center CCAs;
2. identify changes to the ESP, PSP, and CCA security controls to further limit access to CCAs;
3. implement changes identified above; and
4. identify and train any remaining personnel with cyber and unescorted physical access to control center CCAs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002381 CIP-005-1 R1 - OVERVIEW

WECC determined that URE did not identify three Control Center ESP (CORE ESP) access points. WECC determined that URE implemented a "rule change that allowed external access" resulting in the firewalls no longer being isolated within the CORE ESP. Rather, the firewalls became access points to the CORE ESP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not identify the three firewalls as "ESP access points," URE implemented electronic access controls and monitoring at each firewall by virtue of an internal policy requiring firewalls to be protected in a manner consistent with CIP-005 R2. URE's layered security required further authentication before accessing other Cyber Assets within the ESP.

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.

URE submitted its Mitigation Plan designated WECCMIT004842 to address the referenced violations. URE's Mitigation Plan required URE to:

1. validate all current network access points to the ESP, review the current ESP, and check related documentation including access point and network diagrams;
2. update the Control Center ESP plan to reflect new configuration and publish the updated ESP; and
3. update any additional procedures and operational documentation required, including access point administration.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201102851 CIP-005-1 R1; R1.4 - OVERVIEW

WECC determined that URE did not identify at least 15 devices as Cyber Assets within an ESP. The devices were associated with two Critical Assets.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Risk was limited by compensating measures in place during the violation period.

All Cyber Assets were located within a PSP. Although URE did not identify the devices as Cyber Assets, it did afford some logical protection because all of the devices were also located within the ESP. URE's layered security network further limited electronic access to the devices.

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.

URE submitted its Mitigation Plan designated WECCMIT004842 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review process(es) for determining whether electronic assets within the Control Center ESP are Cyber Assets;
2. develop and publish the policy and process for determining whether electronic assets are Cyber Assets;
3. review, update, publish, and implement the process and procedures to introduce and protect new Cyber Assets within a defined ESP based upon the policy developed above;
4. update its list of devices and determine/document which devices on the updated list are Cyber Assets within the Control Center ESP; and
5. submit any required Technical Feasibility Exceptions (TFEs).

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200901633 CIP-005-1 R1; R1.5 - OVERVIEW

WECC determined that URE did not have a documented PRA program for personnel associated with Cyber Assets used in the access control and monitoring of the ESP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had previously performed background screening for its personnel. This violation occurred only because URE did not update these background checks and perform PRAs, as it had not yet completed developing its CIP-004-1 R3 PRA program.

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.

URE submitted its Mitigation Plan designated MIT-09-2002 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002382 CIP-005-1 R2 - OVERVIEW

WECC determined that URE did not document the organizational processes and technical and procedural mechanisms for control of electronic access points at three CORE ESP access points.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although a failure to identify ESPs can render CCAs and associated Critical Assets vulnerable to compromise, a number of compensating factors unique to URE's cyber network in this case lessens the risks. Although URE did not identify the three firewalls as "ESP access points," URE implemented electronic access controls and monitoring at each firewall with an internal policy requiring that all firewalls have protections in a manner consistent with CIP-005 R2. URE's layered security required further authentication before accessing other Cyber Assets within the ESP.

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.

URE submitted its Mitigation Plan designated WECCMIT004843 to address the referenced violations. URE's Mitigation Plan required URE to:

1. validate all current network access points to the ESP, review the current ESP, and check related documentation including access point and network diagrams;
2. update the Control Center ESP plan to reflect new configuration and publish the updated ESP; and
3. update any additional procedures and operational documentation required, including access point administration.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2013013087 CIP-005-3 R3; R3.2 - OVERVIEW

WECC determined that URE did not have a security monitoring process that alerts designated response personnel to unauthorized access attempts and for actual unauthorized access. While URE logged access and access attempts, URE did not provide alerts to appropriate personnel to respond in the event of unauthorized attempts or actual access.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented several physical and logical layers of defense that would likely have prevented and/or detected unauthorized users from logging into any access point protecting CCAs and Electronic Access Control or Monitoring Systems (EACMS). First, URE implemented restricted ports and services and did not allow all traffic to pass through the access points. Second, Intrusion Detection System (IDS) sensors were placed in-line for most access points to the ESP, which would have likely detected any abnormal network traffic or abnormal conditions passing into or out of the ESP. Third, URE has well-trained personnel who monitor network traffic continuously who could have responded immediately to any cyber security attacks or other malicious traffic. Finally, access to the access points is limited to a small group of technicians who must physically be at one of the control centers in order to login and make any type of configuration changes. As such, the probability of someone attempting to login without authorization is extremely limited.

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.

URE submitted its Mitigation Plan designated WECCMIT010947-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify ESP access point events that require automated alerting, at a minimum, to include alerts for login processes;
2. use list of ESP access events to identify gaps in automated alerting and logging processes;
3. create new processes to capture, correlate, and alert on ESP access point logs events;
4. implement any new automated alerting; and
5. train staff on new process.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002269 CIP-006-1 R1; R1.6 - OVERVIEW
WECC determined that on five occasions, URE did not ensure it escorted visitors continuously within the PSP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although visitors were found without their escorts, URE security personnel on site quickly identified visitors and escorted visitors and their escorts from the building. Visitor access to and movement within the site was monitored by video and by URE personnel. Visitors did not have access to CCAs.

WECC determined the duration of the violation to be from when the first unescorted access occurred, through when access was revoked for the last instance of noncompliance.

URE submitted its Mitigation Plan designated MIT-10-3072 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop procedures related to unescorted physical access for use when control centers are staffed with contracted security personnel;
2. provide refresher training;
3. update training program for security personnel;
4. review procedures regarding physical access to and from the loading dock into and out of the building;
5. interview and retrain the personnel at issue;
6. review service contract clauses to ensure authority to take action, including termination, for failing to follow URE policies;
7. provide all contractors with training information related to continuous escort;
8. conduct e-mail outreach regarding continuous escorted access within PSPs;
9. place posters on continuous escorted access near control center entrances;
10. review escort badging process procedures and implement any new requirements;
11. revise system operations hardware maintenance organizations incident response plan to ensure all incidents are referred to URE security;
12. develop alternatives for access modifications to the areas with CCAs in the facility at issue to reduce the size of the PSP;

13. review the visitor access control program for modifications for the reduced sized PSP are warranted;
14. approve the final design(s) for access modifications to the areas with CCAs and proceed with construction;
15. implement the new PSP; and
16. revise internal documents to reflect changes to the visitor access program, implement the changes, and notify all affected employees of the changes.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200901632 CIP-006-1 R1; R1.8 - OVERVIEW

WECC determined that URE's physical security plan did not address a PRA program for personnel associated with Cyber Assets used in the access control and monitoring of the PSP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had previously performed background screening for all its personnel. This violation occurred only because URE did not update these background checks and perform PRAs, as it had not yet completed developing its CIP-004-1 R3 PRA program.

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.

URE submitted its Mitigation Plan designated MIT-09-2001 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002273 CIP-006-1 R4 - OVERVIEW
WECC determined that URE did not implement technical or procedural mechanisms to generate access logs consistent with CIP-006-1 R4 at six PSP access points.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did provide card reader logs for all access points. The building at issue did contain video surveillance as well as security personnel to monitor activity within the building. Further, URE cyber security policy and training prohibited visitor and tailgater access at each of the six access points.

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.

URE submitted its Mitigation Plan designated MIT-09-3120 to address the referenced violations. URE's Mitigation Plan required URE to:

1. consult with URE security and emergency response organization to provide video detection at all of the access points into the facility to ensure that physical access is logged with sufficient information to uniquely identify individuals and to identify tailgaters;
2. select video detection alternative; and
3. complete installation and testing of new equipment.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014618 CIP-006-3c R5 - OVERVIEW
WECC determined that URE did not monitor physical access at all access points to the PSP for approximately 35 hours while its security system was without power.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. When the security system lost power, all access points locked. In order to get through the locked door, personnel were required to contact security to get a combination for a lock box that contained a key to the substation. As a compensating measure, personnel were onsite at various times throughout the outage, thereby shortening the time available for an intruder to cause harm.

WECC determined the duration of the violation to be from when URE failed to continuously monitor access to the PSP, through when URE began continuously monitoring access to the PSP.

URE submitted its Mitigation Plan designated WECCMIT011444-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review and update the physical security response plan with all stakeholders, including identification of stakeholder roles and responsibilities;
2. create detailed procedures, or modify existing procedures, that will align with or support the response plan as required;
3. obtain stakeholder approval for final version of URE response plan;
4. develop change management process to implement for training and awareness on requirements outlined within physical security response plan and stakeholder response plans;
5. execute and complete change management process; and
6. implement physical security response plan and the stakeholder response plans.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801176 CIP-007-1 R1 - OVERVIEW

WECC determined that URE has manual test procedures to test existing security controls. However, due to size and scope of the relevant URE assets, URE failed to determine if any changes affected the security controls of those assets

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintains parallel environments for Critical Cyber Systems with fail-over protection, minimizing the impact of a failure.

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.

URE submitted its Mitigation Plan designated MIT-08-1208 to address the referenced violations. URE's Mitigation Plan required URE to:

1. commission a new tool for security testing;
2. validate proper functioning of the tool;
3. complete automated tests of those assets to form a baseline of existing security controls; and
4. develop procedures to use the new automated tool to test the compliance of systems.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002260 CIP-007-1 R1; R1.1 - OVERVIEW

WECC determined that URE did not create a testing program pursuant to CIP-007 R1 for indicated Cyber Assets and systems; URE failed to test "significant changes" prior to implementation; and URE failed to document any test results. URE failed to create, implement, and maintain a procedure for cyber security testing and failed to examine "rule change" effects on cyber security controls.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Risks posed by noncompliance were, to some extent, reduced given a number of compensating measures in place during the violation period. URE implemented network-scanning tools on segments throughout the ESP in scope. In addition, the ESP has extensive IDS. URE stated that access to an account on its host does not provide access to any relevant domains or hosts, including CCA hosts.

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.

URE submitted its Mitigation Plan designated MIT-08-3474-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify existing technical security controls that could be adversely affected by the addition of a new Cyber Asset or a significant change to an existing Cyber Asset;
2. for controls identified above, identify whether adequate test procedures exist, need to be developed, or existing procedures need to be updated;
3. provide status on development or update of test procedures identified above;
4. complete the development or update of test procedures identified above;
5. train staff on new or updated test procedures;
6. review and update internal documents to require testing of cyber security controls for URE-developed executable code and testing of cyber security controls for third-party software or firmware for new Cyber Assets and for significant changes to existing Cyber Assets within the ESP;

7. review and update existing application-specific test plans to require testing of cyber security controls for URE-developed executable code for new Cyber Assets and for significant changes to existing Cyber Assets within the ESP;
8. review and update the transmission services procedures;
9. provide training for appropriate staff;
10. publish and implement all updated documents; and
11. prepare written report on implementation results.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014628 CIP-007-1 R2 - OVERVIEW

WECC determined that URE did not establish and document a baseline of the ports and services required for normal or emergency operations and ensure that it enabled only those ports and services for 27 devices.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE configured the access points in front of the devices in scope to allow only certain traffic to get to the devices. Even if a port and service were open on a device, the access point might not allow traffic on that port. The access point also is set up to deny all traffic not explicitly allowed in the Access Control List (ACL). URE also uses up-to-date anti-malware that prevents and detects malware attacks designed to compromise the devices. Finally, URE also implemented strong detective controls to detect access to the devices. Specifically, URE uses a security status monitoring utility which could have detected an attempt to compromise the devices.

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.

URE submitted its Mitigation Plan designated WECCMIT011457 to address the referenced violations. URE's Mitigation Plan required URE to:

1. verify that only needed ports and services are enabled, as technically feasible, on the devices in scope of the violation; and
2. update the ports and services documentation for the devices in scope of the violation.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200902261 CIP-007-1 R3; R3.1 - OVERVIEW
WECC determined that URE did not assess or implement 13 patches for three Cyber Assets within 30 days of availability.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE implemented network scanning tools that covered the Cyber Assets in scope. Additionally, the ESP containing Cyber Assets has extensive intrusion detection and protection systems in place. Further, the system host does not provide access to domains or hosts, including CCA operating system hosts.

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.

URE submitted its Mitigation Plan designated MIT-09-3283 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete the assessment of security patches and security upgrades for the open training systems. Document compensating measures to mitigate risk exposure or document acceptance of risk for any patches or upgrades that will not be installed, if any;
2. review remaining software inventory to determine whether security patches or security upgrades were neither installed nor assessed;
3. complete and document the assessment of security patches and security upgrades;
4. for any security patches not installed, either document compensating measures to mitigate risk exposure or document acceptance of risk;
5. review and update security patch process documents as necessary; and
6. provide refresher training on the security patch process.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014629 CIP-007-1 R5 - OVERVIEW
WECC determined that URE did not establish, document, and implement a policy to minimize and manage the scope and acceptable use of factory default accounts for 27 devices.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE had strong preventative controls to prevent unauthorized access. URE implemented a software patch program to ensure that all applicable security-related software patches were installed or, if not installed, had compensating measures to mitigate risk. URE also uses an anti-virus program, which could prevent an attempted malware attack. Additionally, URE implemented a program to enable those ports and services necessary for operation on the access points to the ESP, denying access by default. If a malicious person discovered a vulnerable port and service, malware targeted to only that port would need to pass through the access point, which could stop the attack. In addition, URE implemented strong detective controls to detect unauthorized access. Specifically, URE uses a security testing system that constantly monitors the open ports and services on a device. If a port or service is enabled that is not on the baseline, personnel are alerted, which could allow them to detect a malicious person who is trying to compromise devices on the network. URE is also logging security events on the above devices, which could alert URE to a possible malware attack.

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.

URE submitted its Mitigation Plan designated WECCMIT011456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. examine the default accounts and remove, disable, or rename them where possible. If the account must remain enabled, URE would:
    a. identify individuals who have authorized access to the account;
    b. change the default password per Cyber Asset capability;
    c. enforce minimum password complexity requirements either technically or procedurally; and
    d. enforce password changes at least annually where technically or procedurally feasible.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

<u>WECC201002412 CIP-007-1 R5; R5.2.2 - OVERVIEW</u>
WECC determined that URE did not identify one user with access to a shared account on the Control Center server (a supervisory control and data acquisition (SCADA) server) and failed to change passwords annually for two shared accounts on a second Control Center server.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had security measures in place during the violation period, including access monitoring, logging, and alarming, as well as URE's cyber security training program for all URE employees.

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.

URE submitted its Mitigation Plan designated MIT-09-3531 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review all individual and shared accounts subject to CIP-007 R5;
2. disable the account or identify the individuals with access for all shared accounts for which users with access are not identified;
3. disable the account or change the password for all accounts that have a password older than 13 months;
4. review account management plans for all Cyber Assets subject to CIP-007 R5 and identify which revisions and/or additions to existing annual password change technical and/or procedural controls are necessary;
5. review existing annual user account procedures and identify which, if any, procedures need to be revised to ensure that all individual and shared accounts are addressed;
6. update account management plans to document revisions and/or additions to annual password technical and/or procedural controls, as necessary;
7. update annual user account review procedures, as necessary; and
8. train appropriate staff on revisions and additions to security controls and procedures.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002279 CIP-007-1 R6; R6.4; R6.5 - OVERVIEW

WECC determined that URE did not retain logs of system events related to cyber security for 90 days for a single Cyber Asset, in violation of R6.4. WECC also determined that URE failed to review logs prior to removal, in violation of R6.5.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Access to the Cyber Asset is limited. In addition, the ESP containing the Cyber Asset has no remote access and requires users first to physically access the Control Center PSP before logging into the network. Further, although URE did not maintain logging, the firewall was equipped with alarming which would trigger in the event of logical unauthorized access attempts.

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.

URE submitted its Mitigation Plan designated MIT-09-3284 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document decision to replace management console and firewall appliance;
2. follow established procedures for installing a checkpoint firewall;
3. decommission the management console and the firewall appliance following standard procedures;
4. follow established log management procedures for checkpoint firewalls; and
5. document that logs have been retained for 90 calendar days using the new firewall and perform required review.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has not assessed a penalty for the referenced violation. In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;

2. URE had an internal compliance program (ICP) at the time of the violations which WECC considered a mitigating factor;

3. URE has invested significant time and effort to implement its ICP. WECC considers URE's use of a rapid response team for the self-reporting process to be an exemplary practice. This rapid response team has specific time-based performance targets.

4. URE self-reported the majority of the violations;

5. URE was cooperative throughout the compliance enforcement process;

6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. at no time did any disturbance or outage, or actual harm to the BPS, result from these violations

8. the violation of CIP-002-1 R3 posed a serious or substantial risk to the reliability of the BPS, as discussed above; and

9. 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, no penalty is appropriate.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

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,[5] the NERC

BOTCC reviewed the Settlement Agreement and supporting documentation on December 16, 2015 and approved 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty 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.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

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

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@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.	Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel 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* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
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.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments