October 29, 2015

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 NERC Reliability Standards. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred sixty thousand dollars ($160,000), in addition to other

[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).

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 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 (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
WECC2013012102	CIP-002-1	R3	High/ High	CA	$160,000
WECC2013012387	CIP-003-1	R6	Lower/ Severe	SC	
WECC2012010893	CIP-004-1	R3	Medium/ Severe	SR	
WECC2013012363	CIP-004-2	R4	Lower/ High	SR	
WECC2013012357	CIP-005-1	R1	Medium/ Severe	SR	
WECC2013012459	CIP-005-3	R4	Medium/ Severe	CA	
WECC2013012465	CIP-006-3c	R1, R1.1	Medium/ Severe	CA	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC2013012466	CIP-006-3a	R2, R2.2	Medium/ Severe	CA	$160,000
WECC2014013599	CIP-007-1	R8	Medium/ Severe	SC	
WECC2013012460	CIP-007-3a	R8	Medium/ Severe	CA	

WECC2013012102 CIP-002-1 R3 - OVERVIEW

WECC determined that URE failed to update its list of all Critical Cyber Assets (CCAs) as necessary. Specifically, URE's list of all CCAs contained a number of inaccuracies because URE failed to update the list annually, as required. Further, URE failed to update its master CCA list within 30 days after it decommissioned certain servers.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). All mislabeled and otherwise misidentified devices resided within the Electronic Security Perimeter (ESP) and Physical Security Perimeters (PSPs) and received the logical and physical protections applicable to CCAs. URE appropriately removed the two server devices from service. Physical and logical access to the CCAs is limited to authorized URE personnel who completed personnel risk assessments (PRAs) and cyber security training. URE logs and monitors physical and logical access to the CCAs. Finally, URE personnel are notified of unauthorized access attempts.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE removed the servers from the master CCA list.

URE submitted its Mitigation Plan designated WECCMIT011213 to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the servers from the master CCA list;
2. restructure its change management as it relates to the CCA list;
3. assign additional personnel to assist the CCA list process owner;
4. enhance existing change management procedure to ensure the CCA list is updated prior to testing the change and train resources on the revised procedures and controls;

5. enhance existing information technology NERC CIP implementation checklist to ensure CCA changes are captured; and
6. develop an operational guideline for conducting annual physical asset inventory verification.

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

WECC2013012387 CIP-003-1 R6 - OVERVIEW

WECC determined that URE failed to create change control tickets for patches deployed on Cyber Assets. Approximately half of the devices are classified as CCAs and the remaining devices are electronic access control and monitoring (EACM) devices and Physical Access Control System (PACS) devices, i.e. non-critical Cyber Assets. The devices in scope include printers, workstations, servers, redundant process controllers, scanners, switches, and routers.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because failure to follow change control and configuration management processes for the upgrades could have exposed the CCA hardware and software components to cyber vulnerabilities.

The risk was mitigated because URE does have an established and documented process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software. In addition, URE completed testing on the patches before implementing the patches and gathered and approved testing evidence before it made changes to the devices. Finally, URE's networks are secured, private networks configured specifically to restrict access by default, which do not have access to either URE's intranet or the Internet.

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 WECCMIT010203 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a security management controls document identifying the requirements when change management/ configuration management is needed. The document includes an attachment toolkit containing all the instructions and forms required to complete and finalize a change record;

2. develop several documents to address the deficiencies, including security management control, incident investigations and change management, and a form to initiate the change management process; and
3. conduct a complete and thorough investigation to determine the scope of these incidents and ensure the change management forms are completed correctly and the change management process being followed, by spot checking its management forms pursuant to quality assurance steps.

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

WECC2012010893 CIP-004-1 R3 - OVERVIEW

WECC determined that URE failed to update a PRA at least every seven years for one employee (six days late) and failed to conduct a PRA for ten employees prior to granting physical access to all assets at several facilities. The employees had physical and electronic access to CCAs that included workstations and servers and all assets at these facilities. Eight of the employees in scope also had electronic access to ESPs.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices in scope are equipped with logging and monitoring controls and are located within secure facilities. The employees in scope received cyber security training and did require access to the CCAs. Finally, all employees in scope were employed in good standing by URE and were granted access following completion of their PRAs.

WECC determined the duration of the violation to be from thirty days after the Standard became mandatory and enforceable, through when URE completed the employees' PRAs.

URE submitted its Mitigation Plan designated WECCMIT008115-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. obtain confirmation that the PRAs were completed;
2. change its practice and no longer accept certification letters as PRA evidence—instead requiring a copy of the background investigation; and
3. reinforce practice through communications from management to key staff members.

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

WECC2013012363 CIP-004-2 R4 - OVERVIEW

WECC determined that 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, for approximately a year and a half, URE failed to ensure the performance of quarterly reviews of authorized physical and electronic access to CCAs. In addition, URE did not revoke or update access to its CCAs within seven calendar days for six individuals who no longer required such access.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. While it did not update the access list, URE had manually updated the electronic access for the individuals in the control systems' active directory to reflect new and revoked job responsibilities. Accordingly, the six individuals no longer had electronic or physical access rights to CCAs located within the facilities in scope. Also, the facilities in scope utilize security guards with continuous monitoring and logging, and only qualified and trained personnel with key cards can access these facilities.

WECC determined the duration of the violation to be from eight days after access was first revoked, through when URE updated its access list.

URE submitted its Mitigation Plan designated WECCMIT010178 to address the referenced violations. URE's Mitigation Plan required URE to:

1. submit an access order request to include the affected employee;
2. update the master electronic access list to include the employee's access rights;
3. revise its department procedure relating to CIP-004 R3; and
4. develop stronger controls within that procedure to ensure that information used to perform the 90-day reviews is accurate, and that the electronic access list is updated within seven calendar days of a change. The revised procedure added the following controls:
    a. mandatory use of the access order system for approving and revoking access to NERC CIP facility and CCA;
    b. independent review of the quarterly report;
    c. complete weekly reviews of the electronic access list; and
    d. complete the access worksheet for all access authorizations and revocations.

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

WECC2013012357 CIP-005-1 R1 - OVERVIEW

WECC determined that URE failed to identify a router as an access point to the ESP as required by R1.1 and did not provide the protective measures as outlined in R1.5 to the router and a network-monitoring device. The router is an access point to a data link workstation used to provide real-time operating status to a URE facility. The network-monitoring device functions as a data archival unit and handles alerting as an EACM device.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Only four individuals had electronic access to the router, which URE protected with a non-default password and located within a PSP to which only personnel with approved PRAs and cyber security training had access. In addition, URE protected the network-monitoring device with a defense-in-depth architecture of administrative, physical, and logical cybersecurity controls including physical security mechanisms with guards, special locks, and closed-circuit television (CCTV). Finally, URE implemented logical perimeter and internal cyber security controls, including firewalls, vulnerability scanning tools, and a security and events management system that would immediately identify and alert URE technicians of any unusual event or abnormal behavior.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE updated its related documentation and afforded CIP-005 R1.5 protections.

URE submitted its Mitigation Plan designated WECCMIT010576-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. test the access point to make sure all required controls were in place and functional. Upon successful completion of the testing, URE implemented the access point into the production environment and updated the ESP list, plan, and diagram accordingly;
2. conduct complete due diligence of its ESPs to assure it had accounted for all access points. As a result of this effort, URE was able to merge ESPs;
3. replace the original EACM with new hardware and software, tested the controls, put the device into production, added the device to its asset list and categorized it as an EACM, and updated the network topology and ESP diagrams; and
4. institute all required controls for the firewall manager.

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

WECC2013012459 CIP-005-3 R4 - OVERVIEW

WECC determined that URE could not demonstrate that it performed an adequate Cyber Vulnerability Assessment (CVA) of its ESP access points for three calendar years. URE's annual CVA process utilized a random sampling of Critical Asset sites and a sample of associated Cyber Assets contained at the selected sites.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE did secure its access points within PSPs. In addition, URE implemented technical and procedural controls that limited access via these access points. Finally, URE monitors all ESP access and has implemented defense-in-depth architecture of administrative, physical, and logical cyber security controls, including physical security mechanisms with guards, special locks, firewalls, and CCTV.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE performed a CVA of its electronic access points.

URE submitted its Mitigation Plan designated WECCMIT010568 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets, including EACM and PACS, and document any discrepancies for remediation; and
2. complete its CVA on all Cyber Assets, EACM devices, and PACS.

URE certified that its Mitigation Plan was completed.

WECC2013012465 CIP-006-3c R1, R1.1 - OVERVIEW

WECC determined that URE failed to ensure certain CCAs within an ESP also reside within an identified PSP. The devices were laptop computers that did not reside within an identified PSP and did not have any evidence of alternative measures to control physical access to the devices. The laptops are configuration devices for control systems. The technicians can use the laptops to connect to the devices and provide system programmability to reduce configuration times.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because the violation encompasses all of URE's PSPs and unauthorized access could have been used to harm the operation of the generation facilities. The risk was mitigated because URE continuously monitors all ESP access and has implemented physical security mechanisms with guards, special locks, firewalls, and CCTV. In the event one of the laptops was compromised, electronic monitoring would provide for immediate notification to personnel responsible for response.

WECC determined the duration of the violation to be from the date URE completed the mitigation activities for a prior noncompliance, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010578 to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the original identified devices from NERC CIP scope and retired to the test environment;
2. update documentation and perform data destruction on the devices;
3. add new desktops to the relevant control centers for configuration purposes; and
4. update the documentation to reflect the new desktops.

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

WECC2013012466 CIP-006-3a R2, R2.2 - OVERVIEW

WECC determined that URE failed to identify seven workstations and one server used to authorize access to the PSPs as part of the PACS and failed to afford the PACS devices the protections identified in the Standard. Specifically, URE failed to provide the following protections: 1) the workstations were not segregated from the corporate network and run client software that allows them to communicate with the server in order to authorize physical access to the PSPs; 2) URE did not enable strong technical controls when accessing the PACS server or the PACS network as required by CIP-005 R2.4; 3) URE only required a username and password to access the PACS server from the corporate network; 4) URE failed to implement one or more components of a policy for managing the use of shared accounts that limits access to only those with authorization, an audit trail of account use, and steps for securing the account in the event of personnel change, as required by CIP-007 R5; and 5) URE failed to manage certain shared accounts and afford the shared accounts the protections outlined in CIP-007 R5.2.3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices physically reside within the PSP they were responsible for protecting, thereby receiving continuous physical and electronic monitoring and alarming. The PACS network resides behind the corporate firewall, which URE configured to restrict, monitor, and alert upon suspected malicious activity. Any URE employee that receives access to a shared account must first meet an appropriate business need, obtain approval from an authorized approver, and receive a PRA and mandatory NERC CIP training. Finally, URE reviews individual access to shared accounts quarterly and at any time it revokes access, to ensure shared accounts limit access to only those who are authorized.

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 WECCMIT010577-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. retire the existing PACS and replace with a new PACS in a separate network that does not provide for external, interactive access;
2. enroll the shared accounts in a system enabling URE to maintain audit trails for personnel having access to those shared accounts;
3. submit required TFEs, which have been approved by WECC; and
4. remove all interactive, external access to the relevant servers and installed devices.

WECC2014013599 CIP-007-1 R8 - OVERVIEW

WECC determined that URE failed to perform a CVA on all Cyber Assets within the ESPs at least annually. URE used port scans for a subset of devices and determined there was no need to scan each device since the un-scanned devices were configured identically to the scanned devices. Consequently, URE could not demonstrate that it performed an adequate CVA of all of its Cyber Assets within its ESPs for four calendar years.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because URE may have been unaware of vulnerabilities on the un-scanned devices, such as default or unauthorized accounts. URE also may have been unaware of unauthorized ports and services existing on un-scanned devices.

The risk was mitigated because URE performed a CVA of a sample set of devices and applied any necessary remediation activities to all like devices. URE also performed quarterly log reviews and

would have been alerted to any suspicious activity. In addition, URE performed port comparisons and would have implemented its incident response if it had encountered any unauthorized accounts or ports and services. Also, where technically feasible, all of URE's devices had antivirus installed. Finally, URE had firewalls at the perimeters of its ESPs that are configured to deny by default, which assists in preventing an attacker's ability to enter URE's network.

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 WECCMIT010952 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure's assessment methodology to compare documented baseline ports and services configurations to then-running ports and services configurations for all Cyber Assets;
2. document any discrepancies for remediation; and
3. conduct a CVA on all Cyber Assets pursuant to Standard CIP-007-1 R8.

URE certified that its Mitigation Plan was completed.

WECC2013012460 CIP-007-3a R8 - OVERVIEW

WECC determined that URE failed to perform a CVA on all Cyber Assets within the ESPs at least annually. URE's annual CVA process utilized random sampling of Critical Asset sites and a sample of associated Cyber Assets contained at the selected sites. Consequently, URE could not demonstrate that it performed an adequate CVA of its Cyber Assets within all of its ESPs for three calendar years.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because the violation applied to all of URE's Cyber Assets within ESPs for three years. The risk was mitigated because URE secured its devices utilizing access to ESPs within PSPs. In addition, URE had technical and procedural controls in place that limited access via these Cyber Assets during the violation period and monitors all ESP access. Finally, URE has implemented a defense-in-depth architecture of administrative, physical, and logical cyber security controls including physical security mechanisms with guards, special locks, firewalls, and CCTV.

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 WECCMIT010179 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets, including EACM devices and PACS, and documenting and discrepancies for remediation; and
2. conduct its next CVA on all Cyber Assets, EACM devices, and PACS pursuant to the standard.

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

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred sixty thousand dollars ($160,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations, which WECC considered a mitigating factor;
3. WECC considered the self-reporting of CIP-004-1 R3 as a mitigating factor in penalty determination;
4. 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. the violations WECC2013012102, WECC2013012363, WECC2013012466, and WECC2012010893 posed a minimal risk but did not pose a serious or substantial risk to the reliability of the BPS and violations WECC2013012387, WECC2013012357, WECC2013012459, WECC2013012465, WECC2013012460, and WECC2014013599 posed a moderate risk; 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 sixty thousand dollars ($160,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

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 October 1, 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.

The NERC BOTCC determined that the assessed penalty of one hundred sixty thousand dollars ($160,000) 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.

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

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments