PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 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 NERC and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from NERC's determination and findings of three violations[3] of CIP-007-1. According to the Settlement Agreement, URE admits the violations, and has agreed to the assessed penalty of forty thousand dollars ($40,000), 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 NCEA201200129, NCEA201200130, and NCEA201200131 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

---

[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.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on March 6, 2013, by and between NERC 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
NERC Compliance Enforcement Authority	Unidentified Registered Entity	NOC-1827	NCEA201200129	CIP-007-1	R1.1	Medium	$40,000
			NCEA201200130		R1.2	Lower	
			NCEA201200131		R1.3	Lower	

CIP-007-1

The purpose statement of Reliability Standard CIP-007-1 provides: "Standard CIP-007 requires Responsible Entities[4] 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."

[Footnote added.]

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

CIP-007-1 R1.1, R1.2, and R1.3 provide:

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

CIP-007-1 R1.1 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL). CIP-007-1.2 has a "Lower" VRF and a "Severe" VSL. CIP-007-1 R1.3 has a "Lower" VRF and a "Severe" VSL.

A NERC Compliance Investigation was initiated for an event involving URE (the Event). During the Event, while an information technology (IT) system administrator was installing updated host intrusion protection (HIP) software on URE's energy management system (EMS) workstations in an operations center building, a network loop was created that caused an operational data network (ODN) network storm. During the network storm, the EMS hosts were unable to communicate effectively with system dispatcher workstations and other relevant internal and external parties.

During the first wave of ODN instability, the network storm was localized to a floor of the operations center building. The second wave of ODN instability caused excessive traffic and subsequent

operational failure on another floor ODN switch in the operations center building, which impacted other network ODN traffic. Due to the network failure in the operations center, the EMS application was eventually transferred to a disaster recovery site for EMS approximately four and half hours later. Network operations discovered the data loop the next day, and made network changes to stabilize the network several hours later.

The EMS data outage became system-wide and remained in that state until approximately 15 hours later. From the point the outage became system-wide until approximately 18 hours later, voice recordings and system dispatcher transcripts show the EMS data was intermittently available. After approximately 18 hours from when the outage became system-wide, the network appeared to become stable, and the primary EMS application was returned back to the operations center. During the following hour, network instability again impacted EMS availability because troubleshooting had not been completed successfully. The EMS application was again moved to the disaster recovery site while network troubleshooting resolved the remaining network loops and network storm. The second data outage lasted for approximately an hour and a half on the next day.

Troubleshooting efforts focused on EMS workstations with dual-port network interface cards (NICs) set to "bridging" configuration as a potential cause of the network loops. Redundant links to EMS workstations and servers were disconnected or shut down to return the network to a stable operational state. Additionally, as a precautionary measure, the redundant link between network switches on the two floors of the operations center building was also shut down. Removal of all redundant network connections to dual NICs in the bridging mode resolved the network storm on the one floor (the location of the first wave of ODN instability) and returned the network to a stable state.

During the root cause analysis, URE determined that testing for the patches and updated software was performed in an environment that did not match the production environment. Prior to installation of the updates and patches, testing of the HIP software was completed only on an EMS workstation with a single NIC, but was not tested on EMS workstation configurations with dual NIC cards as some workstations in production were configured. In testing, a "teaming" configuration was utilized while the production system on the day of the event was using a "bridged" configuration on some workstations. In performing the updates and patches, URE did not keep records of its tests. It was confirmed with the vendor of the HIP software that URE should not have installed the software on workstations in a "bridged" network interface.

During the EMS outage, URE system dispatchers relied on the regional control center (RCC) system operators' real time supervisory control and data acquisition (RTSCADA) tools to monitor the URE bulk

power system (BPS). Based on data received from URE, visibility to some of the Remedial Action Schemes (RAS) was lost during the early hours.

NERC determined that URE had a violation of CIP-007-1 R1.1 for failing to develop and follow a specific test procedure for installing and enabling the updates and HIP software associated with this event. This failure resulted in the outage of URE's EMS during the event. While URE stated that the test procedure in this event was used by the system administrator performing the patch procedure to confirm functionality on the EMS test computer prior to rollout to the production workstations, URE had not developed a specific test procedure suitable for testing the updates and HIP software associated with this event.

NERC determined that URE had a violation of CIP-007-1 R1.2 because URE personnel failed to perform testing in a manner that reflected the production environment. Additionally, URE failed to have documentation that showed the testing configuration matched the production configuration.

NERC determined that URE had a violation of CIP-007-1 R1.3 because URE could not provide any evidence that explicit records were kept of the test results performed on the particular EMS test computer prior to the updates and HIP software being installed in this event. Therefore, URE had no evidence to show that it implemented and followed its EMS cybersecurity test procedures.

NERC determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE through when URE completed its mitigation activities.

NERC determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to test new Critical Assets or significant changes to existing Critical Assets within an Electronic Security Perimeter (ESP) presents a risk that installing an upgrade or patch could introduce exploitable vulnerabilities in Critical Cyber Assets and/or other Critical Assets without URE's knowledge. Such vulnerabilities, if exploited, could result in loss of sensitive data, corruption of data, manipulation of applications or data, or complete system failure, thereby placing the reliability of the BPS at risk. In this instance, the violation resulted in the outage of URE's EMS.

These violations also posed a moderate risk to the BPS because the operations documentation in use on the day of the event assumed fully functional and redundant primary and back-up operation center sites. Per URE's effective electric operations document, the EMS second server site, which houses exactly the same set of servers and functionality as the operations center, was supposed to have been

housed in the redundant primary site. Contrary to the electric operations system dispatch back-up procedures, the redundant primary site did not include servers of any kind. On the day of the event, the systems at the disaster recovery site were not in their normal and tested state per URE's own specification and were being dismantled to be transferred to the redundant primary site to set up the post-transition configuration of the redundant primary site. The state of this site on the day of the event is unknown, and following the dismantling of the dual equipment to transfer parts of it to the redundant primary site, the remaining system at the disaster recovery site was not tested and was not proven to be capable of taking on the production role.

The risk to the BPS was mitigated by the following factors. URE dispatchers did have some data to monitor the BPS during the event. The URE dispatchers at the redundant primary site used this intermittent data to monitor and control the BPS. In addition, URE transmitted this intermittent data to WECC and another entity for their use to fulfill their reliability obligations.

Compliance Enforcement Authority's Basis for Penalty

According to the Settlement Agreement, NERC has assessed a penalty of forty thousand dollars ($40,000) for the referenced violations. In reaching this determination, NERC considered the following factors:

1. URE's compliance history was not considered an aggravating factor;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which NERC considered a mitigating factor;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. The violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
6. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, NERC determined that, in this instance, the penalty amount of forty thousand dollars ($40,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[5]

URE's mitigating activities to address its violations of CIP-007-1 were submitted to NERC as complete.

URE took the following actions to mitigate the violation and prevent recurrence:

1. Deployed a dual NIC configuration in the EMS workstations. The vendor confirmed that a dual NIC architecture provides the most robust and redundant environment for critical EMS workstations and servers;
2. Conducted a configuration audit of all EMS workstations to identify any bridged NICs;
3. Partnered with the vendor, Intel, and obtained updated drivers and software that allows the NICs to operate in a teamed configuration;
4. Tested the new drivers and teaming software in its quality assurance (QA) environment, and then installed the teaming software and drivers on all workstations configured in bridged mode, thereby eliminating bridging completely;
5. Installed the dual NIC cards and teaming software on the production workstations in the control room at the redundant primary site, replacing the configuration of the two single NIC cards;
6. Implemented a new checklist to provide contingency validation of the operating system health as well as special case checks where necessary;
7. Used dual NICs to provide the workstation with a layer of redundancy to the network. Each NIC interface is connected to separate switches. In the event of a single network switch failure, the workstation will maintain connectivity to the network via the redundant connection and the EMS system;
8. Reviewed all dual NIC systems to ensure that "bridged" mode was configured to "teaming" mode to eliminate single points of failure and provide the redundancy expected with this configuration;
9. Performed physical walk downs of all cable connections on the two floors in the operations center, specifically auditing network connections. Technicians validated switch port descriptions and updated as applicable, in addition to labeling telecom blocks with switch and port assignments;

[5] *See* 18 C.F.R § 39.7(d)(7).

10. Upgraded the internetwork operating system (IOS) on its ODN switches to improve overall security and stability of network and enable enhanced feature capability. URE identified IOSs which would be applicable for the environment, conducted performance testing in its network lab, and scheduled and implemented IOS upgrades. The IOS upgrades improved capability to reduce the risk of spanning tree loops in the network infrastructure. In addition, URE has partnered with vendors to review IOS versions and provide recommendations to consider for future upgrades and additional feature functionality to further protect the network infrastructure;
11. Improved network topology which leverages a hub/spoke design, rather than daisy chain connections; and
12. Implemented additional redundancy for the entire EMS. The EMS multi-host configuration has been put into place. If the systems drop off-line due to a network failure at one site, the EMS systems will automatically failover to the redundant site.

URE certified that the above mitigating activities were completed. As evidence of completion of its Mitigation Plan, URE submitted the following documents:

1. A document providing the confirmation from the vendor that a dual NIC architecture provides the most robust and redundant environment for critical EMS workstations and servers.
2. A document providing the change request to upgrade NIC drivers on dual NIC workstations and install "teaming" configuration in place of "bridging" configuration.
3. A document providing the change request to restore the two floors network connections to original configuration.
4. The documents providing the review and updating of the change management process and standards for EMS, RAS, and SCADA workstations and servers. This includes testing of representative desktop specific configurations when operating system patches or new/updated applications are installed.
5. A document providing the investigation and inventory of the EMS, SCADA, and RAS computing infrastructure to ensure that "bridging" configuration is not enabled on either workstations or servers.
6. A document identifies, verifies and documents network cabling on the two floors.
7. A document providing evidence of the upgrade of IOS on the switches on the two floors.

8. A document providing the spanning tree enhancements to network switches in order to minimize the potential for network loops.

After reviewing URE's submitted evidence, NERC verified that URE's mitigating activities were completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2013. The NERC BOTCC approved the Settlement Agreement, including NERC's assessment of a forty thousand dollar ($40,000) 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. NERC reported that URE was cooperative throughout the compliance enforcement process;
2. URE had a compliance program at the time of the violation which NERC considered a mitigating factor, as discussed above;
3. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. NERC determined that the violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
5. NERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

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

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of forty thousand dollars ($40,000) 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 NERC and URE executed March 6, 2013, included as Attachment a;

    a. Disposition of Violation, included as Attachment a to the Settlement Agreement;

b) NERC Final Compliance Investigation Report, included as Attachment b; and

c) URE Mitigation Completion Document, included as Attachment c.

A Form of Notice Suitable for Publication[8]

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

[8] *See* 18 C.F.R § 39.7(d)(6).

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	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 of Enforcement Processing 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Sean Bodkin* Associate Counsel and Manager, Enforcement Actions North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3022 (202) 644-8099 – facsimile sean.bodkin@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/ 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 of 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
North American Electric Reliability Corporation

Attachments