PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 30, 2011

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Abbreviated Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP11-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Abbreviated Notice of Penalty (NOP) regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violation[1] discussed in detail in the Disposition Document attached hereto (Attachment a), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This NOP is being filed with the Commission because URE does not dispute the violation of CIP-006-1 R1.8 and the assessed zero dollar ($0) penalty. Accordingly, the violation identified as NERC Violation Tracking Identification Number MRO201000157 is a Confirmed Violation, as that term is defined in the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violation

This NOP incorporates the findings and justifications set forth in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) issued on November 4, 2010, by the

[1] 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.

[2] *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 (2010). *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).

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Midwest Reliability Organization (MRO). The details of the findings and the basis for the penalty are set forth in the Disposition Document. This NOP filing contains the basis for approval of this NOP by the NERC Board of Trustees Compliance Committee (BOTCC). In accordance with Section 39.7 of the Commission's Regulations, 18 C.F.R. § 39.7, NERC provides the following summary table identifying each violation of a Reliability Standard at issue in this NOP.

NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Duration	Total Penalty ($)
NOC-711	MRO201000157	CIP-006-1	1.8	Lower[3]	7/1/09 – 4/10/10	0

The text of the Reliability Standard at issue and further information on the subject violations are set forth in the Disposition Document.

CIP-006-1 R1.8 - OVERVIEW

MRO determined that URE did not install an appropriate use banner, make automated alerting available, review the ninety day log for user account access activity, review or disable the ports and services, apply security patches, install anti-virus, remove default administrative accounts, back up the system configuration, or submit the appropriate Technical Feasibility Exceptions (TFE).

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 NOCV and supporting documentation on January 10, 2011. The NERC BOTCC approved the NOCV and the assessment of a zero dollar ($0) financial penalty against URE based upon MRO's findings and determinations, the NERC BOTCC's review of the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violation at issue.

In reaching this determination, the NERC BOTCC considered the following factors:[6]

1. the violation constituted URE's first violation of the subject NERC Reliability Standard;

[3] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" Violation Risk Factor (VRF) and CIP-006 R1.7, R1.8 and R1.9 each have a "Lower" VRF.
[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).
[6] MRO did not consider URE's compliance program as a factor in determining the penalty, as discussed in the Disposition Document.

2. URE self-reported the violation;
3. MRO reported that URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. MRO determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), as discussed in the Disposition Document; and
6. MRO reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC believes that the assessed penalty of zero dollars ($0) 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 NOP with the Commission, or, if the Commission decides to review the penalty, upon final determination by the Commission.

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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Attachments to be included as Part of this Notice of Penalty

The attachments to be included as part of this NOP are the following documents:

a) Disposition of Violation and Verification of Mitigation Plan Completion therein, dated January 10, 2011, included as Attachment a;

b) URE's Self-Report dated March 23, 2010, included as Attachment b;

c) URE's Mitigation Plan, MIT-09-2785, submitted August 16, 2010, included as Attachment c;

d) URE's Certification of Mitigation Plan Completion dated August 16, 2010, included as Attachment d; and

e) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction dated November 2, 2010, included as Attachment e.

A Form of Notice Suitable for Publication[7]

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

[7] *See* 18 C.F.R. § 39.7(d)(6).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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 David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, NJ 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net Daniel P. Skaar* President Midwest Reliability Organization 2774 Cleveland Avenue North Roseville, MN 55113 651-855-1731 dp.skaar@midwestreliability.org Sara E. Patrick* Director of Regulatory Affairs and Enforcement Midwest Reliability Organization 2774 Cleveland Avenue North Roseville, MN 55113 651-855-1708 se.patrick@midwestreliability.org	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@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.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this NOP as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ *Rebecca J. Michael*

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Sr. Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Midwest Reliability Organization

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment a

Disposition of Violation and Verification of Mitigation Plan Completion therein, dated January 10, 2011

DISPOSITION OF VIOLATIONS[1]

Dated January 10, 2011

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.	NOC#
MRO201000157	**MRO201000157**	**NOC-711**

REGISTERED ENTITY
Unidentified Registered Entity (URE)

NERC REGISTRY ID
NCRXXXXX

REGIONAL ENTITY
Midwest Reliability Organization (MRO)

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-006-1[2]	**1**	**1.8**	**Lower[3]**	**Severe[4]**

PURPOSE OF THE RELIABILITY STANDARD AND TEXT OF RELIABILITY STANDARD AND REQUIREMENT(S)/SUB-REQUIREMENT(S)

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

CIP-006-1 R1.8 provides:

> **R1. Physical Security Plan — The Responsible Entity [5] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> **…**

---

[1] For purposes of this document and attachments hereto, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[2] This standard was amended on December 16, 2009 by NERC, and as of October 1, 2010 can be found in its amended state under CIP-006-3.

[3] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" Violation Risk Factor (VRF) and CIP-006 R1.7, R1.8 and R1.9 each have a "Lower" VRF.

[4] At the time of the violations, no VSLs were in effect for CIP-006-1 R1.8. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications."

[5] Within the text of Standard CIP-006-1 R1.8, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> **R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.**
>
> **...**

(Footnote added.)

VIOLATION DESCRIPTION

On March 23, 2010, URE self-reported noncompliance with Reliability Standard CIP-006-1 R1.8. URE's access control system that controls and monitors physical access to the Physical Security Perimeter (PSP) for the data center and control room PSPs was not afforded the following protective measures required by Reliability Standard CIP-006-1 R1.8:

1. **Appropriate use banner was not installed.**
   a. **Reliability Standard CIP-005-1 R2.6 states that "[w]here technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner."**
   b. **On April 7, 2010, MRO Compliance Staff confirmed that the appropriate use banner was not installed on the PSP server. MRO determined this after inquiring with URE Subject Matter Experts (SMEs) and by reviewing the PSP diagram provided by URE.**
2. **Automated alerting was not available and a Technical Feasibility Exception (TFE) had not been submitted.**
   a. **Reliability Standard CIP-005-1 R3.2 states that:**
      "[w]here technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days."
   b. **On April 7, 2010, MRO Compliance Staff confirmed that automated alerting was not available for the access control system.**
3. **The ninety day log review of user account access activity was not completed between July 1, 2009 and March 18, 2010.**
   a. **Reliability Standard CIP-007-1 R5.1.2 states that "[t]he Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days."**

b. Reliability Standard CIP-007-1 R6.4 states that "[t]he Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days."
c. Reliability Standard CIP-007-1 R6.5 states that "[t]he Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs."
d. On April 7, 2010, MRO Compliance Staff confirmed that the ninety day log review was not completed between July 1, 2009 and March 18, 2010. The ninety day log review was completed on March 19, 2010. The log was not reviewed because the log file on the PSP server was not set to the proper size.

4. Ports and services were not reviewed and disabled and a TFE had not been submitted.
   a. Reliability Standard CIP-007-1 R2 states that:

      "Ports and Services -- The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
      R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
      R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
      R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk."

   b. On April 7, 2010, MRO Compliance Staff confirmed that ports and services were not reviewed and disabled and a TFE had not been submitted.
5. Security patches were not applied and a TFE had not been submitted.
   a. Reliability Standard CIP-007-1 R3 states that:

      "Security Patch Management -- The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
      R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
      R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document

compensating measure(s) applied to mitigate risk exposure or an acceptance of risk."

b. On April 7, 2010, MRO Compliance Staff confirmed that security patches were not applied and a TFE had not been submitted.

6. Anti-Virus was not installed and a TFE had not been submitted.
   a. Reliability Standard CIP-007-1 R4 states that:

      "Malicious Software Prevention -- The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

      R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

      R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures."

   b. On April 7, 2010, MRO Compliance Staff confirmed that Anti-Virus was not installed and a TFE had not been submitted.

7. Default administrative accounts were not removed until March 19, 2010.
   a. Reliability Standard CIP-007-1 R5 states that:

      "Account Management -- The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

      R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed."

   b. On April 7, 2010, MRO Compliance Staff confirmed that the default administrative accounts for accessing the access control system were not removed until March 19, 2010.

8. The system configuration was not backed up.
   a. Reliability Standard CIP-009-1 R4 states that "[t]he recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc."
   b. Reliability Standard CIP-009-1 R5 states that "[i]nformation essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

c. On April 7, 2010, MRO Compliance Staff confirmed that system configuration was not backed-up URE lacked back-up media.

Therefore, MRO concluded that URE did not afford protective measures for all Cyber Assets used in the access control and monitoring of the PSP as required by CIP-006-1 R1.8.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

MRO determined that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) and only posed a minimal risk because the cyber asset subject to this violation only communicates with the card reader system and is wholly isolated from URE's corporate network, Supervisory Control and Data Acquisition (SCADA) system, and the internet. The cyber asset and its connections are located within the PSP and cannot be accessed by any external sources. Furthermore, URE's facilities are manned 24 hours per day, and 7 days per week.

IS THERE A SETTLEMENT AGREEMENT YES ☐ NO ☒

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT	YES	☐
ADMITS TO IT	YES	☒
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS)	YES	☐

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT	YES	☒

II. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S) **7/1/09 (when URE was required to be compliant with the standard) through 4/10/10.**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **3/23/10**

IS THE VIOLATION STILL OCCURRING
YES ☐ NO ☒
IF YES, EXPLAIN

REMEDIAL ACTION DIRECTIVE ISSUED YES ☐ NO ☒
PRE TO POST JUNE 18, 2007 VIOLATION YES ☐ NO ☒

III. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-09-2785**
DATE SUBMITTED TO REGIONAL ENTITY	**8/16/10**
DATE ACCEPTED BY REGIONAL ENTITY	**8/16/10**
DATE APPROVED BY NERC	**9/1/10**
DATE PROVIDED TO FERC	**9/1/10**

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE
N/A

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE **3/31/10**
EXTENSIONS GRANTED **N/A**
ACTUAL COMPLETION DATE **3/31/10**

DATE OF CERTIFICATION LETTER **8/16/10**[6]
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF **3/31/10**

DATE OF VERIFICATION[7] **8/31/10**
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF **3/31/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

URE has taken the following actions to mitigate the issue and prevent recurrence:

1. **Conducted a detailed investigation to determine steps to bring the cyber asset into strict compliance;**
2. **Reviewed accounts and disabled manufacturer and default guest accounts;**
3. **Reviewed logs and confirmed that they were retained for 90 days. URE also submitted a TFE request;**
4. **Installed appropriate use banner on the server;**

[6] The Mitigation Plan cover page states that the entity certified completion of the Mitigation Plan on August 31, 2010.
[7] This Disposition Document serves as MRO's Verification of Mitigation Plan Completion.

5. **Contacted MRO regarding the steps to report a possible violation of the CIP Standards. URE also submitted a TFE request;**
6. **Reviewed and documented ports, services and compensating measures. URE also submitted a TFE request;**
7. **Confirmed that Anti-Virus could not be installed on the server. URE also submitted a TFE request;**
8. **Confirmed that Security Patches were not installed on the server due to age of the application and mitigation measures were in place. URE also submitted a TFE request;**
9. **URE submitted a TFE to document the compensating measures in place for manual review of account log in lieu of automated alerts;**
10. **Ordered, received, and installed backup equipment;**
11. **Completed full backup for covered assets;**
12. **Completed third party vulnerability assessment (covered cyber assets were included); and**
13. **Established a new statement of work for assistance with the establishment and monitoring of recurring tasks associated with CIP-002 through CIP-009.**

MRO reviewed the evidence and documentation submitted by URE and on August 31, 2010 verified completion of the Mitigation Plan as of March 31, 2010. Where technically feasible, URE has afforded its Cyber Assets used in the access control and monitoring of the PSP the protective measures specified in Reliability Standard CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, CIP-007, CIP-008, and CIP-009.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

1. **Scope of work schedule, dated June 7, 2010**
2. **TFE Request for CIP-005-1 R3.2**
3. **TFE Request for CIP-007-1 R2.3**
4. **TFE Request for CIP-007-1 R3**
5. **TFE Request for CIP-007-1 R4**
6. **TFE Request for CIP-007-1 R6**

IV. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$0** FOR **ONE** VIOLATION OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

PREVIOUSLY FILED VIOLATIONS OF ANY OF THE INSTANT RELIABILITY STANDARD(S) OR REQUIREMENT(S) THEREUNDER
YES ☐ NO ☒

LIST VIOLATIONS AND STATUS
N / A

ADDITIONAL COMMENTS
N / A

PREVIOUSLY FILED VIOLATIONS OF OTHER RELIABILITY STANDARD(S) OR REQUIREMENTS THEREUNDER
YES ☐ NO ☒

LIST VIOLATIONS AND STATUS
N / A

ADDITIONAL COMMENTS
N / A

(2) THE DEGREE AND QUALITY OF COOPERATION BY THE REGISTERED ENTITY (IF THE RESPONSE TO FULL COOPERATION IS "NO," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

(3) THE PRESENCE AND QUALITY OF THE REGISTERED ENTITY'S COMPLIANCE PROGRAM

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐
EXPLAIN
URE has a compliance procedure which was in place at the time of the violation. MRO did not consider this procedure a factor in determining the penalty.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

EXHIBITS:

SOURCE DOCUMENT
URE's Self-Report submitted March 23, 2010

MITIGATION PLAN
URE's Mitigation Plan, MIT-09-2785, submitted August 16, 2010

CERTIFICATION BY REGISTERED ENTITY
URE's Certification of Mitigation Plan Completion submitted August 16, 2010

VERIFICATION BY REGIONAL ENTITY
This Disposition Document serves as MRO's Verification of Mitigation Plan Completion

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: **10/15/10** OR N/A ☐

SETTLEMENT DISCUSSIONS COMMENCED
DATE: OR N/A ☒

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: **11/4/10** OR N/A ☐

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒

REGISTERED ENTITY RESPONSE
ACCEPTED ☒
DATE: **11/2/10**
OR
CONTESTED ☐
DATE:
FINDINGS ☐ PENALTY ☐ BOTH ☐

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED