November 25, 2014

**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 Entities, FERC Docket No. NP15-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), and Unidentified Registered Entity 3 (URE3), (collectively, the UREs), NERC Registry ID# NCRXXXXX , NCRXXXXX, and 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 Midwest Reliability Organization (MRO), on behalf of itself, Southwest Power Pool Regional Entity (SPP RE), and Western Electricity Coordinating Council (WECC), and the UREs have entered into a Settlement Agreement to resolve all outstanding issues arising from MRO's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the UREs do not contest the violations and have agreed to the assessed penalty of one hundred and fifty thousand dollars ($150,000) in addition

[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 (2014). *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) and 18 C.F.R § 39.7(d).

[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.

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 in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

**Statement of Findings Underlying the Violations**

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. 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 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

| NERC Violation ID | Reliability Standard | Req. | VRF/ VSL* | Applicable Function(s) | Total Penalty |
|---|---|---|---|---|---|
| MRO2012009882 | CIP-003-2 | R5; R5.1.1; R5.1.2; R5.2; R5.3 | Lower/ Severe | The UREs | $150,000[4] |
| MRO201100289 | CIP-003-1 | R6 | Lower/ Severe | URE1, URE3 | |
| MRO201100323 | CIP-004-2 | R3; R3.1; R3.2 | Medium/ High | URE1, URE3 | |
| MRO201100322 | CIP-004-1 | R4; R4.1 | Lower/ High | URE1 | |

[4] MRO shall divide the penalty amount in three parts based on the relative net energy for load of each Regional Entity.

| NERC Violation ID | Reliability Standard | Req. | VRF/ VSL* | Applicable Function(s) | Total Penalty |
|---|---|---|---|---|---|
| MRO2012010698 | CIP-004-3 | R4; R4.1; R4.2 | Lower/ High | The UREs | $150,000 |
| MRO201100287 | CIP-005-1 | R1; R1.5 | Medium/ Severe | The UREs | |
| MRO2012009900 | CIP-005-1 | R1; R1.5; R1.6 | Medium/ Severe | The UREs | |
| MRO201100288 | CIP-005-1 | R5; R5.1; R5.2 | Lower/ Severe | URE1, URE3 | |
| MRO201100325 | CIP-006-1 | R1; R1.2; R1.3; R1.7 | Medium/ Severe | URE1 | |
| MRO2012009899 | CIP-006-1 | R1; R1.8 | Lower/ Severe | The UREs | |
| MRO2012011501 | CIP-006-1 | R1; R1.8 | Lower/ Severe | The UREs | |
| SPP2012010242 | CIP-006-1 | R1; R1.8 | Lower/ Severe | The UREs | |
| MRO201100290 | CIP-006-3a | R2; R2.1; R2.2 | Medium/ Severe | The UREs | |
| MRO2012010967 | CIP-006-3c | R4 | Medium/ Severe | URE1 | |

| NERC Violation ID | Reliability Standard | Req. | VRF/ VSL* | Applicable Function(s) | Total Penalty |
|---|---|---|---|---|---|
| MRO2012010966 | CIP-006-3c | R6 | Lower/ Severe | URE1 | $150,000 |
| SPP2012010241 | CIP-007-1 | R3 | Lower/ Severe | URE1 URE2 | |
| MRO201000232 | CIP-007-1 | R5; R5.2.3 | Medium/ Severe | URE1, URE3 | |
| MRO2012009992 | CIP-007-1 | R5; R5.3.1; R5.3.2; R5.3.3 | Medium/ Severe | The UREs | |
| MRO201100292 | CIP-007-1 | R7; R7.1; R7.2 | Lower/ Severe | URE1, URE3 | |

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

The UREs notified MRO that they had identified several compliance concerns and would be conducting a comprehensive review of their CIP compliance program. The UREs submitted multiple Self-Reports to MRO, SPP RE, and WECC. Also during this time, MRO conducted a CIP Compliance Audit of URE1, while SPP RE and WECC jointly conducted a CIP Compliance Audit of URE2 and URE3. MRO reports that, throughout the process of conducting their comprehensive review, the UREs have been actively communicating and meeting with staff from MRO, SPP RE, and WECC.

This Settlement Agreement includes 19 violations:

1. eight violations processed by MRO on behalf of MRO, SPP RE, and WECC;
2. five violations processed by MRO on behalf of MRO and WECC;
3. four violations in the MRO region only; and
4. two violations processed by SPP RE on behalf of MRO, SPP RE, and WECC.

CIP-003-2 R5 (R5.1.1, R5.1.2, R5.2, R5.3) (MRO2012009882)

URE1 submitted a Self-Certification to MRO stating it was in violation of CIP-003 R5. URE2 and URE3 also reported noncompliance with the same standard and requirement to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to implement their program for managing access to protected Critical Cyber Asset (CCA) information.

The UREs conducted a survey to identify CIP information, determine whether the information was classified appropriately, and determine whether or not it was protected in compliance with CIP requirements and the UREs' CIP information protection program. The survey results identified that several CIP information repositories (electronic file locations) used to store CIP protected information did not have all the necessary access controls in place.

The UREs' CIP information protection program required that all CIP protected information be stored in a specified folder structure within a repository for which the required controls were in place. The UREs' CIP protected information was also being stored in other repositories that did not have all required access controls in place. Additionally, the UREs identified nearly 10% of users with incorrect access privileges to protected information.

MRO determined that the UREs had a violation of CIP-003-2 R5 for failing to implement their program for managing access to protected CCA information.

MRO determined the duration of the violation to be from the first date CIP protected information was found to reside in a repository without the required access controls through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). The UREs control multiple BPS facilities. The violation continued for two years and involved nearly 10% of all user accounts and several unauthorized repositories. Examples of repositories that were not subject to the access controls specified in CIP-003 R5 included network drives, internal document sharing sites, and other internal non-approved document management systems accessible by multiple individuals that were not part of the UREs' CIP program. Examples of protected documents stored in the unapproved repositories included CIP policies and procedures, physical access control system programming information, security plans and drawings, Technical Feasibility Exception (TFE) working documents, and shared password change evidence. Further, the UREs overall information protection program was found to be inadequate.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. revise the CIP access control program to include the CIP-003 R5 requirements necessary to secure and protect CIP information repositories;
2. train all CIP information repository owners and administrative support staff on the revised CIP access control program;
3. require each repository owner and administrative support staff to document the process and procedures for controlling access to his or her respective repository or security group;
4. require each repository owner and administrative support staff to review the user access privileges for his or her respective repository or security group to confirm that they are correct and that they correspond with the appropriate business need-to-know requirement;
5. remove access for any individuals that no longer required access; and
6. identify CIP information repositories that store CIP protected information and add the repository owners, titles, and name of the repository for which they approve access to the designated approver personnel list.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-003-1 R6 (MRO201100289)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-003-1 R6. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

Specifically, URE1 and URE3 (collectively, the UREs) failed to follow their substation change control process to ensure all CCAs were subjected to the change control and configuration management program, for both changes to existing CCAs and the addition of new devices into existing Critical Asset environments. This failure resulted in the inconsistent identification and tracking of new CCAs and an inconsistent application of the UREs' change control and configuration management program.

The Self-Report was the result of an internal inventory conducted by the UREs of Cyber Assets within the Electronic Security Perimeter (ESP) of BPS substations. The internal assessment identified discrepancies between CCAs contained on lists maintained by URE1 and URE3 and those deployed in the field. After further review, the UREs determined that certain BPS substation CCAs commissioned

or decommissioned after a certain date had not been handled in a manner consistent with the UREs' substation change control and configuration management process.

The UREs identified multiple instances of changes to substation CCAs subject to CIP-003-1 R6 where they failed to follow their process for change management. Of the total number of changes, most involved the addition of new CCAs to a substation. The UREs failed to follow the required configuration management and change control process and appropriately update documentation. These CCAs included primary and secondary line relaying, bus differential relaying, and breaker failure relaying at substations. The UREs also failed to follow their change management process for CCAs, including substation protective relays that underwent modification or retirement.

This violation was also the root cause of additional self-reported violations of CIP-005-1 R5 (MRO201100288) and CIP-007-1 R7 (MRO201100292).

MRO determined that the UREs had a violation of CIP-003-1 R6 for failing to follow their substation change control process to that ensure all CCAs were subjected to their change control and configuration management program.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the UREs' newly-added CCAs were not properly documented upon installation and not properly included in the UREs' CIP compliance program. Therefore, they were not ensured protection under the CIP Reliability Standards. Without proper protections, these CCAs were vulnerable and could potentially have been exploited. The CCAs were located at critical high-voltage substations and Interconnection Reliability Operating Limit flow gates. Further, the duration of the violation was over two years.

However, several factors mitigated the risk posed by the violation. The change control issue was limited. Although the changes did not follow the additional requirements for CCAs, the UREs followed their standard testing, checkout, and commissioning process, which provided substantial security controls. None of the changes were related to the electronic access management system, which provided primary remote access security control for the substations affected by the violation. The process weakness that allowed this violation was not present for this system. Lastly, the UREs did not experience any issues with their energy management systems (EMS) during the pendency of the violation.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the pre-commissioning checklist;
3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement it by starting use of the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;
9. inform MRO of status of contacting the other utilities; and
10. execute an additional action plan to augment the substation change control process and resolve the remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-004-2 R3 (R3.1, R3.2) (MRO201100323)

During the MRO Compliance Audit, MRO determined that URE1 had a violation of CIP-004-2 R3 for failing to ensure that all employees with authorized cyber access to CCAs and unescorted physical access to CCAs had an identity verification. MRO discovered that one employee did not have a

complete Personnel Risk Assessment (PRA) in place for five months because the PRA did not include an identity verification.

A comprehensive review was conducted across the UREs. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

As a result of the internal review, the UREs identified a total of four individuals whose PRA dates fell outside the seven-year required period. For two individuals, access was removed and eventually restored. One individual had access removed and was notified of the screening requirement. One individual was a contractor who no longer required access.

Additionally, the UREs identified seven individuals who had not undergone an identity verification as required by CIP-004-2 R3.1. Two of the individuals did not have identification verifications because they had security freezes on their social security numbers. One of the seven individuals was a foreign national, and the UREs did not perform a passport verification. Additionally, three of the seven individuals had high levels of electronic and physical access rights to Critical Assets.

MRO determined that the UREs had a violation of CIP-004-2 R3 for failing to conduct PRAs with identity verifications and for failing to update each PRA at least every seven years.

MRO determined the duration of the violation to be from the earliest date a PRA was noncompliant through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the UREs perform multiple functions across multiple BPS facilities. Three of the individuals that did not have identity verification had high levels of access rights. One of the individuals was a foreign national for whom the UREs did not perform a passport verification.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

The UREs' Mitigation Plan required the UREs to:

1. update the master access list;
2. conduct a review of current PRA procedures to define further steps for conducting, reviewing, and reporting PRAs;
3. add an annual audit of the UREs' CIP master access list to the UREs' CIP procedures to ensure the PRAs are current and complete; and

4. review the PRA of each individual with CIP access to ensure they are current and complete, with seven-year criminal checks and identity verifications.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (MRO201100322)

During the MRO Compliance Audit, MRO determined that URE1 was in violation of CIP-004-1 R4. URE1 failed in three instances to update the list of its personnel who have authorized cyber or authorized unescorted physical access to CCAs within seven calendar days of any change. Specifically, two employees and one contractor had a change in job responsibilities, but URE1 did not update its list until over 20 days, over six months, and nearly one year later, respectively.

MRO determined that URE1 had a violation of CIP-004-1 R4 for failing to update its list of personnel who have access to CCAs within seven calendar days of any change.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 through when URE1 completed its Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Each of the three individuals continued to work at URE1. Each of the individuals retained the need for access, but that need was not documented. In addition, each of the individuals maintained up-to-date cybersecurity training and PRAs during the violation period.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. analyze, design, and implement an interim manual process to manage access control;
2. design a long-term, automated solution that automates the process of managing temporary or indefinite access needs upon employee/contractor status change (as identified from the human resources information system).
3. review and test the request form process workflow;
4. create a process to obtain a validation from the individual's manager for continued access upon any human resources information system change;

5. develop a new automated process to compare the human resources information system daily changes with the master access list. If an individual is found with a change and is on the master access list, the system will require validation to maintain access;
6. test enhancements;
7. communicate the new process to all managers; and
8. update related documentation to support the new process.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (R4.1, R4.2) (MRO2012010698)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-004-3 R4. URE2 and URE3 reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

Specifically, URE1, URE2, and URE3 (collectively, the UREs) failed to review quarterly the list of personnel with access to CCAs, update the list within seven calendar days of any change of personnel, and remove logical or unescorted physical access to CCAs within seven calendar days for personnel who no longer required such access.

The UREs identified less than one percent of individuals who did not have unescorted physical access to CCAs removed within seven days, as specified by CIP-004-3 R4. The unescorted physical access to CCAs was removed between 11 and 50 days from the change in status. The UREs' records indicate that none of the five individuals actually accessed any facility containing CCAs after their change in status.

The UREs also noted that URE3 failed to revoke physical access to URE3 CCAs for four individuals employed by a third-party entity that had access to URE3 substations. Access was removed for these four individuals between ten days and seven months after the change in status. None of the status changes were terminations for cause. A representative from the entity disclosed to URE3 that it had not always taken the proper steps to notify URE3 of the individuals' change in status. Without that notice, URE3 was unable to revoke access for terminations and transfers on a timely basis.

Additionally, the UREs noted that there was a lack of reliable connectivity between the UREs' physical access control system and card readers at particular URE3 and URE1 substations containing CCAs. As a result, six individuals (two for URE1 and four for URE3) were able to continue accessing those substations after their physical access was revoked in the physical access control system for periods

ranging from twelve days to six months. Because the individuals' access was removed in the physical access control system, they were not on the master access list, and their access was not reviewed on a quarterly basis.

Lastly, the UREs identified one instance where an employee transferred to a new job within the company and needed to retain access rights for a period of about two months after the transfer. The UREs failed to respond to an automated email alerting individuals of a need of change in access.

MRO determined that the UREs had a violation of CIP-004-3 R4 for failing to review quarterly the list of personnel with access to CCAs, update the list within seven calendar days of any change of personnel, and remove logical or unescorted physical access to CCAs within seven calendar days for personnel who no longer required such access.

MRO determined the duration of the violation to be from when the first individual's access was removed in the physical access control system but the individual still retained access at the card readers through when the UREs executed an agreement with the third-party entity mentioned above to monitor access to the UREs' CCAs.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The instances of access were for short durations involving individuals who had PRAs and had received the required cybersecurity training. In the instance where the transferred employee's access was not timely revoked, the employee's PRA and cybersecurity training were current. The inadequate process was limited to employee transfers. Other staffing changes such as terminations included all of the required information within the notification. Additionally, the communication issue between the physical access control system and card readers was limited to substations with low bandwidth communication.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. enhance the personnel change request form, which serves as official notification of a change in employee status, to include an area to identify whether the employee is a CIP employee. This change will allow for prioritization these forms;
2. develop and implement a disciplinary process to enhance management awareness of the importance of these forms;

3. implement a configuration update to the forms to hard code notifications to the appropriate departments, regardless of whether an invalid email address is manually entered on the form;
4. hold a meeting with the employees who are assigned to manage access to CIP-restricted areas to determine if there may be access control process and procedure efficiencies at the substations at issue;
5. hold a discussion with the third-party entity representative who manages CIP access controls to discuss the entity's commitment to implementing changes to prevent similar violations from occurring in the future;
6. implement a more formal agreement with the third-party entity, which will transition coordination with the entity and access control processes to the individuals who have more direct oversight of all individuals with authorized unescorted access to the CIP restricted area(s) within their respective locations;
7. review each site, individually and as a whole, to identify the root cause of the intermittent connectivity issue with the physical access control system and card readers. Staff tested solutions and implemented them at the affected sites; and
8. develop a monitoring and reporting tool to notify the UREs' security staff, which monitors the physical access control system, of any sites that have not connected. This report is sent every six hours.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R1 (R1.5) (MRO201100287)

URE1 submitted a Self-Report to MRO stating it was in violation of CIP-005-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP. These Cyber Assets consisted of a class of servers used to monitor, alarm, and log access to CIP substation ESPs. This system is used to access multiple Critical Assets and multiple CCAs.

The UREs failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, as required by CIP-007-1 R6. Due to incorrectly configured disk space overwrite settings, the UREs failed to perform a review of security event logs. When this

issue was discovered, the UREs took a snapshot of the active log data. From the snapshot log, the UREs found that the logs were incomplete and did not provide continuous security event data over the relevant time period. An in-depth analysis of the log generation and review process also identified a secondary automated script failure issue related to a previous upgrade in the scripting tool.

During mitigation, the UREs determined that there were additional issues with the servers as well as dial-up devices used to authenticate calls to the substation. The UREs failed to review or address certain alarm logs generated by both systems. The UREs failed to develop and implement testing procedures for evaluating adverse impacts of the security controls for the servers, as required by CIP-007-1 R1.

The UREs also failed to change shared passwords annually for the servers, as required by CIP-007-1 R5.3.3.

For URE1 and URE2, the UREs failed to perform a Cyber Vulnerability Assessment (CVA) for one year on these systems, as required by CIP-007-1 R8. Furthermore, in another year's CVA, the UREs failed to verify a list of ports and services required for operation were enabled, as required by CIP-007-1 R8.2.

MRO determined that the UREs had a violation of CIP-005-1 R1 for failing to afford several of the protective measures specified in R1.5 to Cyber Assets used in the access control and monitoring of the ESPs.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The UREs did not conduct an effective CVA in one year, and they did not remediate issues identified in the next year's CVA. As referenced in the CIP-003-1 R6 (MRO201100289) violation, the UREs did not implement CIP documentation change control during installation of the devices. During a CVA, the UREs discovered that they failed to maintain a list of certain ports and services, and they failed to remediate this issue by the following year's CVA. However, the risk posed by this violation was mitigated by several factors. Specifically, the UREs maintained a test environment and test procedures which specified a back-out plan for each change. While the UREs did not specifically test for adverse impacts on security controls, all changes had readily available plans to reverse any change that degraded security controls. Further, access to the affected system was only available through the UREs' corporate network, which then provided access to substations through a dedicated modem.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it was complete.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change two EMS shared account passwords;
3. design, develop, and test a manual log review process, review portions of the security event logs using the new manual process, and train the relevant team on the new manual log review process;
4. assess security monitoring processes for the devices to specifically address recipients of current automated alerts, action (response) plans for each recipient, and any other associated automated alerts;
5. change physical access control system and monitoring/logging server passwords for shared accounts where doing so did not pose unacceptable adverse impacts;
6. complete the investigation and verification for shared password accounts in the CIP environment;
7. complete the review and updating of policies, processes, and procedures to reflect accurate and up-to-date controls that address CIP-007 R5;
8. update process and procedure documentation to reflect responsibilities, actions performed, documentation created, and notifications made as part of the log review process;
9. investigate the ability to perform automated detection and alerting for issues affecting the log backup process;
10. draft action (response) plan for security events/alerts for affected devices, defining security event (rules with thresholds), response/action plan roles and responsibilities, and response action(s), among other items;
11. identify cybersecurity controls to be verified when a significant change is made. Controls to be verified include items such as audit log settings, password requirements, running services/open ports, default accounts, and so on;
12. communicate and train administrators on any changes to the processes and procedures to comply with CIP-007 R5;
13. complete the CVA action plan's last remaining item related to the affected devices, which was to investigate the ability to restrict access to a port on a modem;

14. finalize security event response (action) plans, update current processes and procedures, and draft communications to impacted teams;
15. consider and evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
16. test approved changes made to alerting processes;
17. develop process and procedure to compare established security controls before and after a significant change has been applied;
18. verify that all affected devices were identified and included within the scope of a subsequent year's CVA;
19. implement all approved changes and communicate to the appropriate resources;
20. select and retain consultant to perform and complete CVA of affected systems;
21. communicate and train administrative personnel on the process and procedure regarding determinations of whether cybersecurity controls are negatively affected by a significant change;
22. implement pilot test of long-term solution;
23. communicate and train administrators on the new tool, process, and procedure for shared password accounts;
24. implement test procedures to include verification that security controls in the monitoring/logging systems are not adversely affected by a change; and
25. implement long-term solution to improve management of shared password accounts within CIP environment and resolve remaining non-compliant shared account.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R1 (R1.5, R1.6) (MRO2012009900)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-005-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

Specifically, URE1, URE2, and URE3 (collectively, the UREs) failed to ensure that Cyber Assets used in the access control and/or monitoring of the ESPs were afforded the protective measures as specified in Standard CIP-007-1 R3 (patch management) and CIP-007-1 R5 (account management).

While gathering evidence to demonstrate that applicable security patches had been tracked, evaluated, tested, and installed for all Cyber Assets within the ESPs, the UREs discovered that non-Microsoft security patches were not included in the discovery and assessment phase of security patch management for some servers. The UREs had a patch management program in place to ensure applicable security patches are installed on these systems; however, non-Microsoft applications were not included within the scope of that program. The UREs did not properly assess patches for nearly 60 percent of the devices (the remaining applications had no patches over the period). Of those applications, the UREs' assessment deemed none of the patches applicable to the UREs' configuration.

Additionally, the UREs identified that a number of shared system accounts associated with the affected systems did not have all the necessary access controls in place as required by CIP-007-1 R5.1.3, CIP-007-1 R5.2.3, and CIP-007-1 R5.3 (see MRO201000232 and MRO2012009992).

The UREs reported the following: 1) shared system accounts, along with the name and title of the personnel who authorize access, were not maintained on a designated approvers list prior to a certain date; 2) documented access control procedures did not exist for managing access to these shared systems accounts and no annual reviews of the documented access controls had been performed; and 3) evidence of annual user access reviews did not exist. Further, some shared account owners did not identify a list of authorized users or maintain a usage log (audit trail) for their accounts. Additionally, some database shared account passwords were not changed annually. Mitigation was required for multiple user accounts, with two-thirds of those resulting in the account being deemed unnecessary and consequently removed.

In addition, the UREs later reported that they had discovered numerous changes that were made at Critical Asset substations. Simultaneous with reporting this information related to the instant violation, the UREs also submitted a Self-Report indicating that it was in violation of CIP-003-1 R6 (see MRO201100289). The UREs installed and modified Critical Asset substation ESP access points without subjecting them to a change control and configuration management process, resulting in these systems

not being tested for security controls prior to installation. Specifically, one substation ESP access point was replaced at a Critical Asset substation, and three new ESP access points were installed at new Critical Asset locations. None of the four changes was done in accordance with the UREs' change control and configuration management program. Because the change control and configuration management program was not followed, there was no documentation related to these ESP access points and no security controls testing was conducted prior to commissioning.

MRO determined that the UREs had a violation of CIP-005-1 R1 for failing to ensure that systems used in the access control and monitoring of the ESPs were afforded each of the protective measures specified in R1.5.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, there were a high number of accounts with incorrect access privileges. The UREs were unaware of which individuals had access and had not reviewed access or maintained logs. The UREs did not have adequate patch management procedures for the substation electronic access points, and they had incorrect documentation of the software baseline of the substation ESP devices. The UREs was not properly testing substation electronic access points for security controls when changes were made. There were several hundred CCAs that could be accessed using the electronic access points. Individuals would have had the ability to control BPS elements accessible through these points.

However, the risk was mitigated by the following factors. The only method to access the electronic access points at issue was from the UREs' network, which required authentication.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. complete an inventory of all applications that reside on the affected monitoring/logging servers to determine which applications are necessary and which can be removed;
2. assign responsibilities for the remaining applications to various URE groups to ensure that new security patches are discovered, assessed, and documented;
3. remove any unnecessary applications from the servers, following the UREs' change control process, and apply applicable security patches to necessary applications;

4. develop a procedure to discover, assess, and document new security patches regularly;
5. conduct a gap assessment to identify all shared, generic, or administrative accounts with access to the monitoring/logging application and servers;
6. develop training materials and train all affected account owners on the access controls and remediation required to bring all accounts into compliance with CIP-007 R5 requirements and subsequent CIP access control program;
7. have each account owner document his or her respective access control process and procedures for his or her respective account(s);
8. have each account owner review the user access privileges for his or her respective account(s) to confirm that they are correct and that they correspond with the appropriate business need to know;
9. assess, identify, and implement a solution for annual password changes for the database service accounts and update procedures and program documentation;
10. add the accounts to the designated approver personnel list along with the account owner's name and title; and
11. regarding test procedures, complete and document mitigating activities as part of the Mitigation Plan for MRO0201100289.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R5 (R5.1, R5.2) (MRO201100288)

URE1 submitted a Self-Report stating that it was in violation of CIP-005-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

Specifically, during an internal inventory of substation Cyber Assets, URE1 and URE3 (collectively, the UREs) identified discrepancies between listed Cyber Assets and those deployed in the field. After further review, the UREs determined that certain substation ESP access points commissioned or decommissioned after a certain date had not been handled in a manner consistent with the UREs'

substation change control and configuration management process. As a result, the UREs failed to update documentation within 90 days of the change in two instances.

MRO determined that the UREs had a violation of CIP-005-1 R5 for failing to review, update, and maintain all documentation to support compliance with the requirements of CIP-005.

MRO determined the duration of the violation to be from the date when the UREs failed to update their documentation within 90 days as required by CIP-005-1 R5.2 through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This issue was limited to two 115 kV BPS facilities. In both cases, the devices that were installed were dial-up appliances that allowed remote access to CCAs with no routable connectivity outside the facility. The devices were accessible only from the UREs' corporate network through a special server used to communicate with the dial-up devices. Therefore, it was not likely that the installation of these devices would have an adverse impact on the security of the CCAs.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the UREs' pre-commissioning checklist;
3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;

9. inform MRO of status of contacting other utilities; and
10. execute the additional action plan to augment the substation change control process and resolve the remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.2, R1.3, R1.7) (MRO201100325)

During the MRO Compliance Audit, MRO determined that URE1 was in violation of CIP-006-1 R1. Specifically, URE1 failed to ensure and document that all Cyber Assets within an ESP also resided within an identified Physical Security Perimeter (PSP). MRO discovered several PSPs which failed to incorporate a completely enclosed six-wall border.

In one facility, MRO identified an opening in the six-wall border above the double doors leading from the main hallway into the PSP.

At another facility, MRO identified a non-continuous six-wall border a mechanical room.

MRO also determined that the physical security plan did not accurately reflect the current PSP configuration. URE1 relocated an access point and the access point's associated card reader. The changes undertaken as part of this project resulted in the redefinition of the PSP boundary. These changes were not listed in a version of the physical security plan over 30 days following the conclusion of the project. Therefore, MRO determined that the physical security plan was not updated within thirty days.

MRO determined that URE1 had a violation of CIP-006-1 R1 for failing to create and maintain a physical security plan that met all of the requirements of the standard.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 through when URE1 completed its Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PSP was within a secured building with security guards, surveillance cameras, and non-CIP card readers. The undocumented PSP configuration changes were properly documented approximately four months later. Both PSP openings were partially obstructed by conduit, wiring, and ductwork and were relatively small.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. improve CIP restricted area diagrams and replace existing diagrams with architectural drawings;
2. create a checklist that incorporates steps to update the physical security plan for each CIP restricted area;
3. complete an inspection of each CIP restricted area to identify, inspect, and ensure that a continuous six-wall perimeter is clearly defined and intact for each identified CIP restricted area;
4. provide a documented checklist that demonstrates that six-wall perimeters have been inspected;
5. create a document to be utilized each time a CIP restricted area has been identified as a construction project that may/may not change the PSP;
6. review the work order template and identify an area for a drop-down box that indicates work is adjacent or inside a CIP restricted area;
7. correct identified deficiencies in six-wall borders; and
8. submit work orders to the construction group to identify construction materials needed to ensure a continuous six-wall border for both PSPs and to complete the tasks as described in the work orders.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (MRO2012009899)

URE1 submitted a Self-Report to MRO stating it was in violation of CIP-006-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-006-1 R1 to Cyber Assets used in the access control and monitoring of the PSP.

The UREs failed to assess non-Microsoft patches (such as those for anti-malware software, backup software, and utilities) for their Cyber Assets that authorize and/or log access to their PSPs as required by CIP-007-1 R3. The UREs also failed to have all necessary access controls and procedures in place for

shared accounts on these same Cyber Assets, as required by CIP-007-1 R5.2. In addition, the UREs did not maintain evidence of annual user account access reviews, maintain a list of authorized users for shared accounts, enforce annual password changes, or maintain an audit trail for the shared accounts associated with these Cyber Assets, as required by CIP-007-1 R5.2.

Upon further review, the UREs discovered that they made numerous changes to PSP devices without following the CIP change control and configuration management process, as required by CIP-003-1 R6 (see also MRO201100289).

MRO determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protective measures specified in CIP-006-1 R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The UREs have multiple BPS facilities. The UREs had a high number of unnecessary accounts and accounts with incorrect access privileges. All of the shared accounts on these devices had compliance deficiencies: two-thirds of the accounts were removed, and the other one-third required some level of remediation. The UREs failed to review access or maintain adequate logs. The UREs had inadequate knowledge of the software baseline of their PSP devices or the procedures needed to patch these systems. The UREs did not have an inventory of installed software applications for devices used in the access control and monitoring of the PSPs. Of the "patchable" applications found on the UREs' PSP devices, the UREs failed to assess nearly 25% (although the UREs' assessment determined that none of the patches were applicable to their configuration).

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. document all installed applications on the physical access control system servers;
2. perform gap assessment for all accounts on the physical access control system application, database, and servers to identify business need for all generic, administrative, and shared accounts and determine gaps in access controls, and prepare report on findings;
3. assess and determine a solution for database service account annual password changes;

4. develop training plan for account owners, identify personnel, draft training materials, and schedule training dates;
5. develop a shared database password change remediation plan;
6. determine which applications are necessary to support critical functions and which applications could be removed from the servers;
7. determine which group is responsible for the discovery, assessment, and documentation of security patches for each application on the servers and assign ownership;
8. train relevant personnel on CIP-007 R5 access control requirements;
9. update the designated approver personnel list with the approvers and the associated accounts;
10. perform an access needs assessment for accounts;
11. establish a procedure to discover, assess, install, and document new security patches for assigned applications on a periodic basis;
12. assess, and if applicable, test, document, and install patches to bring applications up to date;
13. implement the database service account password changes;
14. submit appropriate requests to remove or modify accounts;
15. implement patch discovery, assessment, and implementation procedures on an on-going basis;
16. document CIP account access control procedures for the accounts in scope;
17. revise CIP access control program document to address or further clarify the requirements of CIP-007 R5; and
18. document the results of the account remediation plan, including, but not limited to, what accounts were remediated and what accounts were removed or disabled.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (MRO2012011501)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-006-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which was consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures specified in CIP-006-1 R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

The UREs discovered that their physical security vendor made a change to their physical access control system without following the UREs' change control and configuration management process, as required by CIP-003-1 R6. The vendor also failed to ensure that significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls, as required by CIP-007-1 R1. The UREs did not perform any testing procedures as required by CIP-007-1 R1 when installing an update to two of the associated servers.

The UREs also discovered that a number of database user roles within their physical security system were mapped to security groups within the UREs' physical security system, but were not documented by the UREs, and the database user roles did not have passwords assigned to them as required by CIP-007-1 R5.2.

MRO determined that these issues were caused by a lack of communication with the UREs' physical security vendor and a lack of understanding by the UREs of their physical security system's configuration (which was installed by the vendor).

MRO determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protections specified in R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The UREs have multiple BPS systems, and the systems at issue had the ability to control physical access to all of the UREs' CCAs. The database user roles issue involved multiple, separate security groups and several active directory security groups associated with the UREs' physical security system. There were two accounts that had full access to the database for installation and configuration modification to all of the UREs' physical access control system. One of these accounts had inadvertent access for about a year. However, the risk posed by this violation was

mitigated by several factors. The vendor personnel who used the two accounts that had full access to the database had valid PRAs and cybersecurity training. Further, the risk associated with the update for a single change was minimal. Follow-up testing did not reveal any additional issues with the way the change was implemented, and the UREs did not identify any other instances of this issue.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. perform an access review on each identified security group and remove unnecessary access;
2. determine and implement security event monitoring and update associated documentation; and
3. update the designated approver personnel list and access control documents with information related to remaining security groups.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (SPP2012010242)

During the Joint Compliance Audit, SPP RE and WECC determined that URE2 and URE3 (collectively, the UREs) were in violation of CIP-006-1 R1. The UREs did not identify certain workstations used to provision access rights and to monitor alarms as physical access control system assets; therefore, the UREs could not provide evidence that the workstations were afforded all protective measures specified in CIP-006-1 R1.8.

The audit team found that unnecessary ports and services were enabled on certain URE3 physical access control system panel devices.

The audit team also found that antivirus signature files were not tested by the UREs before being implemented on the physical access control systems, as required by CIP-007 R4.2. The UREs asserted that they were relying upon the antivirus vendor to have tested the signature files before being published and that the risk of malware in the corporate network environment necessitated the immediate deployment of the anti-virus signature files upon receipt. This violation was determined to apply to URE1, URE2, and URE3.

SPP RE determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protective measures specified in R1.8 to Cyber Assets used the access control and monitoring of the PSPs.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs until mitigated.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not affording all protections according to CIP-006-1 R1.8 to the workstations, there was a risk that the physical access control system could have been compromised, leading to unauthorized access to CCAs. Having unnecessary ports and services enabled on the physical access control system panels devices presented the risk that a malicious actor might disable or render the panel devices inoperable. Because antivirus signature files were only tested in the vendor's environment, which is not representative of the UREs' environment, there was a risk that the UREs' ability to monitor and control their environment would have been affected upon installation of the signature files.

However, the risk was mitigated by the following factors. The workstations physically resided within a controlled-access area, and electronic access to the workstations was restricted to authorized users. The workstations were subject to the enterprise patch management program and were guarded by up-to-date anti-malware software. The UREs had disabled the unnecessary ports and services on the physical access control system panels following a CVA. Further, a failure of the physical access control system will not cause a loss of physical access control. Card readers will continue to authenticate access using the latest local database in the door control panels. Should the workstation used to provision access fail, access rights will not be able to be changed until the workstation is restored, but existing access rights will be preserved and used. A failure of the workstation used to monitor door alarms will result in loss of alarm monitoring ability on the affected workstation; however, there is redundancy, and the primary PSPs are manned at all times. No actual harm occurred to any of the UREs' Cyber Assets as a result of the violation.

The UREs' Mitigation Plan to address this violation was submitted to SPP RE.

The UREs' Mitigation Plan requires the UREs to:

1. replace the workstations with terminal server(s) and configure them for restricted access by appropriate personnel;
2. disable all unnecessary ports and services on the physical access control system panels that control CIP PSPs;

3. conduct a port scan to validate that all unnecessary ports were disabled;
4. establish a process to test the anti-malware signature files distributed by the UREs' anti-malware vendor;
5. review security/access controls to ensure the terminal servers comply with all applicable requirements of CIP-006-3 R2.2;
6. transition security operations center personnel from using local physical access control system clients to the terminal server client and ensure that all necessary functionality is available; and
7. remove the local installation of the physical access control system client from the local workstations.

CIP-006-3a R2 (R2.1, R2.2) (MRO201100290)

URE1 submitted a Self-Report stating it was in violation of CIP-006-3 R2. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-006-3a R2.2 to Cyber Assets that authorize and/or log access to the PSP.

The UREs failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, as required by CIP-007-3 R6. The UREs did not perform a review and analysis of Windows security event logs for the Cyber Assets that authorize and/or log access to the PSP. During a quarterly log review, the UREs discovered that the security event log was missing. The UREs' physical access control system servers were determined to have incorrectly configured disk space overwrite settings. An in-depth analysis of the UREs' log generation and review process also identified a secondary automated script failure issue related to a previous upgrade in the scripting tool.

After reviewing a snapshot of current logs, the UREs determined that the logs were incomplete due to a Windows log overwrite feature. The snapshot log did not provide continuous security event data over the relevant time period. During a preliminary review certain quarterly logs, the UREs also identified gaps in the Windows security logs.

During mitigation of the self-reported violations and the Joint Compliance Audit, the UREs determined that there were additional issues with the physical access control system. The UREs failed to develop and implement testing procedures for evaluating adverse impacts to the security controls for the

physical access control system. The UREs failed to change shared passwords for the system annually, as required by CIP-007 R5.3.3. Additionally, the UREs determined that a CVA was not performed for one calendar year on the system, as required by CIP-007 R8.

MRO determined that the UREs had a violation of CIP-006-3a R2 for failing to afford several of the protective measures in CIP-006-3a R2.2 to Cyber Assets that authorize and/or log access to the PSP.

MRO determined the duration of the violation to be from the first day of the quarter when the UREs were unable to review the previous quarter's security event logs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The physical access control system was used to monitor and control access to all of the UREs' PSPs. When the UREs performed a CVA, it discovered a "high risk" action item for the system's administrator accounts. Further, the UREs did not have a baseline list of approved ports and services for Cyber Assets used in the access control and monitoring of PSPs. Therefore, MRO determined that the failure to develop or implement test procedures, change shared account passwords, and conduct a CVA presented a serious or substantial risk to the reliability of the BPS.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it was completed.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change two EMS shared account passwords;
3. design, develop, and test manual log review process, review portions of quarterly security event logs using the new manual process, and train the relevant team on the process;
4. identify cybersecurity controls to be verified any time a significant change is made;
5. update process and procedure documentation to reflect responsibilities, actions performed, documentation created, and notifications made as part of the log review process;
6. investigate the ability to perform automated detection and alerting for issues affecting the log backup process;
7. correct all shared accounts discovered to be non-compliant where doing so does not pose unacceptable adverse impacts;

8. complete the investigation and verification for shared password accounts in the CIP environment;
9. complete the review and updating of policies, processes, and procedures to reflect accurate and up-to-date controls that comply with CIP-007 R5;
10. communicate and train administrators on changes to the processes and procedures to comply with CIP-007 R5 standard;
11. address three action items from the CVA, including correcting documentation to reflect a server determined to be needed for operation, removing a documented server no longer needed, and compiling list of approved services;
12. consider and evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
13. create process and procedure to compare established security controls before and after a significant change has been applied;
14. create a non-production test environment for the physical access control system application so that all desired changes can be tested for functionality and impact to cybersecurity controls prior to implementing change into the production environment;
15. communicate and train administrative personnel on the process and procedure;
16. communicate and train administrators on the new tool, process, and procedure for shared password accounts to ensure compliance with CIP-007;
17. implement test procedures to include verification that security controls in the physical access control systems are not adversely impacted by a change; and
18. implement long-term solution to improve management of shared password accounts within CIP environment and resolve remaining shared account at issue.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-3c R4 (MRO2012010967)

URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R4. URE1 failed to implement operational controls to manage physical access at all access points to the PSP at all times.

URE1's security personnel responded to a door alarm. Upon investigating the alarm, URE1 discovered that the employee pulled the door open without utilizing his badge, which serves as a unique identifier. Investigating further, the employee was observed leaving the area and tampering with the door latch to keep the door from securing when he left. Less than a minute later, when the same employee returned, he was able to enter the area without logging his access. At the time of re-entry, the latch was also returned to normal so the door would secure behind him.

MRO determined that URE1 had a violation of CIP-006-3c R4 for failing to implement operational controls to manage physical access at all access points to the PSP at all times.

MRO determined the duration of the violation to be for a brief time on the date when URE1 failed to implement operational controls to manage physical access.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The door latch was disabled for a short period of time, and the individual was in close proximity to the door while outside of the PSP. Additionally, URE1's physical access monitoring mechanisms were functioning properly at the time of the incident; the issue was identified because opening the door without first swiping a key card triggered the "forced door" alarm. Further, the facility at issue was continuously manned, and the operators could see the door from their stations. Also, the employee that tampered with the door had authorized, unescorted access to CCAs, had a current PRA, performed the required cybersecurity training prior to the incident, and had a valid business justification to be in the area.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it was completed.

URE1's Mitigation Plan required URE1 to:

1. place signs at access points stating that everyone must run his or her ID badge on the card reader;
2. have site management emphasize proper access controls; and
3. have the employee's manager confer with the individual employee responsible for the violation.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-006-3c R6 (MRO2012010966)

URE1 submitted a Self-Report stating it was in violation of CIP-006-3c R6. URE1 failed to log sufficient information to uniquely identify individuals and the time of access at all times. URE1 reported that it identified five separate occasions on which employees entered a designated PSP and did not comply with URE1's access control procedures, resulting in URE1's failure to log their access.

The first of the five instances occurred when URE1's security personnel responded to a door alarm. Upon investigating the alarm, URE1 discovered that an employee pulled the door open without using his badge, which served as a unique identifier. Investigating further, the employee was observed leaving the area and tampering with the door latch to keep the door from securing when he left. Less than a minute later, when the same employee returned, he was able to enter the area without logging his access. At the time of re-entry, the latch was also returned to normal so the door would secure behind him.

URE1's security personnel completes weekly "tailgating" assessments to ensure accurate and complete access logs. An individual engages in "tailgating" when he or she follows another individual with authorized access into a controlled access area without passing his or her badge by the card reader; as a result, the second individual's access is not logged. To complete the assessments, employees review access history reports and verify via camera that there is only one individual entry per card read or that the manual access log is utilized.

On one day, security personnel was completing a tailgating assessment and discovered two instances of tailgating. On two separate occasions, an employee with access to the area followed another individual into a facility without running his/her badge on the access control reader.

On a subsequent date, security personnel was completing another tailgating assessment and discovered two instances of tailgating. On two separate occasions, employees who had access to the area followed another individual into the area without running his/her badge on the access control reader.

MRO determined that URE1 had a violation of CIP-006-3c R6 for failing to implement the technical and procedural mechanisms for logging physical entry at all access points to the PSPs.

MRO determined the duration of the violation to be from the date URE1 first failed to uniquely identify individuals and the time of access through the date of the last instance and when URE1 resumed logging sufficient information.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In all five instances, the employees had authorized, unescorted access to CCAs, had a current PRA and cybersecurity training, and had a valid business justification to be in the controlled access area. In the instance where an employee tampered with the door lock, the facility was continuously manned, and the operators could see the door from their stations. Additionally, URE1 discovered the noncompliance through its proactive review process, promptly reported the issue to MRO, and has increased its awareness efforts.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. engage in discussions with the managers of the employees, including security services staff, regulatory/compliance staff, and human resources staff. Since these discussions, management reinforced proper access controls with their entire facility staff; and
2. contact the managers of the individuals by the URE1 department responsible for recommending the level of discipline, and complete the disciplinary processes with the individuals responsible for the violations.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-007-1 R3 (SPP2012010241)

During the Joint Compliance Audit, SPP RE discovered that URE2 was in violation of CIP-007-1 R3. URE2 did not establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within its ESP.

Subsequently, the UREs performed a review of all Cyber Assets within the facility ESPs across all operating regions to identify any Cyber Assets not being managed in accordance with CIP-007-1 R3. In total, URE2 failed to include six Cyber Assets within an ESP in a patch management program, and URE1 failed to include over 20 Cyber Assets within an ESP in a patch management program. As a result, URE2 and URE1 (collectively, the UREs) failed to assess for applicability three patches associated with

five URE2 Cyber Assets and nearly 40 patches associated with 10 URE1 Cyber Assets. Two of the patches associated with URE1 Cyber Assets addressed software vulnerabilities.

SPP RE determined that the UREs had a violation of CIP-007-1 R3 for failing to include a number of Cyber Assets within ESPs within their patch management programs.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Out-of-date security patches could have allowed for unauthorized electronic access to, and potential compromise of, Cyber Assets within the ESPs. Such potential compromise could have resulted in a loss of monitoring or control capabilities for the UREs' facilities. Upon discovering the missing patches, the UREs performed an assessment and installed those patches that were applicable and necessary. Further, two of the missed patches addressed security issues. However, all other patches were optional in nature, as they were enhancements or addressed bug-fixes. None of the affected Cyber Assets were CCAs, and all of the affected assets resided within PSPs. All of the affected Cyber Assets were logically protected behind ESP firewalls requiring network access and authentication for remote access. None of the affected assets showed degradation of function from the failure to install patches, and there were no instances of malware or ESP-network intrusion.

The UREs' Mitigation Plan to address this violation was submitted to SPP RE.

The UREs' Mitigation Plan required the UREs to:

1. assess the patches that were missed and apply those that were deemed necessary;
2. review CIP-007-3 R3 security patch management with EMS personnel to ensure they understand the importance of security patch management;
3. review the security patch management process for all EMS team-controlled Cyber Assets to ensure the proper steps are fully documented;
4. identify opportunities for improvement in processes and collection of evidence to meet requirements and apply improvements to the security patch management process;
5. review, train, and reinforce the new processes and evidence requirements with staff in order to meet CIP requirements;
6. perform regular security patch management improvement validation on a sampling of patches to determine that evaluations are being performed in a timely manner.

The UREs certified that the above Mitigation Plan requirements were completed. SPP RE verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R5 (R5.2.3) (MRO201000232)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-007-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

URE1 and URE3 (collectively, the UREs) failed to implement a policy for managing the use of accounts that limits access to only those with authorization and secures the account in the event of personnel changes, as required by CIP-007-1 R5.2.3.

The UREs reported that they failed to change shared account passwords in accordance with their policy based on the risk identified with the shared account passwords. The UREs' EMS account management policy provided for a shared account password to be changed within seven days if an individual with access to that account was terminated (unless the termination is for cause), or had a change in assignment in which he or she no longer needed access to the shared account.

However, in two instances where employees with access to EMS shared accounts resigned or retired, the UREs did not change the shared account passwords within seven days. The shared accounts at issue were for the EMS platform. In the first instance, the EMS user account employee resigned but the password was not changed until nearly three weeks later. In the second instance, an EMS administrative account user retired and the password was not changed until six months later.

The UREs' personnel with system administrator responsibilities had access to all of the functions within the EMS through a shared administrative account. For some individuals, the shared EMS administrative account could be accessed remotely through the corporate network or directly from certain consoles.

Although the shared passwords were not changed in accordance with the company policy, the two individuals at issue had no means of remotely accessing their EMS accounts seven days after their last date of employment with the company. Although the individuals could have accessed the EMS accounts by being physically at the CCA itself, the physical access for these individuals was revoked on their respective last days.

The UREs reported that the failure to change shared passwords arose because of a gap between the requirements of their policy and the specific procedure to implement the policy.

MRO determined that the UREs had a violation of CIP-007-1 R5 for failing to implement their policy for minimizing and managing the scope and acceptable use of administrator, shared, and other generic account privileges.

MRO determined the duration of the violation to be from when the UREs first failed to change the shared account password within the required seven days through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Since the individuals had their remote access credentials revoked, their only method of accessing the EMS administrative account would have been to either be physically at the server (which resided within a PSP to which they no longer had access) or to compromise the credentials of another employee.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change the shared account passwords;
3. complete investigation and verification for shared password accounts in the CIP environment;
4. complete corrective action for shared accounts discovered at issue;
5. review and update policies, processes, and procedures to reflect accurate and up-to-date controls that address CIP-007 R5;
6. communicate and train administrators on changes to the processes and procedures;
7. evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
8. implement pilot test of long-term solution;
9. communicate and train administrators on the new tool, process, and procedure for shared password accounts to ensure compliance with CIP-007; and
10. implement long-term solution to improve management of shared password accounts within CIP environment.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R5 (R5.3.1, R5.3.2, R5.3.3) (MRO2012009992)

URE1 submitted a Self-Report stating it was in violation of CIP-007-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing. URE1 and URE3 (collectively, the UREs) failed to ensure that CCA passwords were changed at least annually.

URE1's EMS has a number of communication front-end (CFE) assets that facilitate communication with the EMS. There are four domain accounts set up to serve all of these CFEs. Only designated personnel with system administrator responsibilities have access to these accounts. URE1 discovered that EMS personnel had not changed the passwords on the four CFE asset accounts annually, resulting in non-compliance with CIP 007-3 R5.3.3. Upon discovery, the CFE passwords were changed.

URE3 discovered that EMS personnel had not changed the passwords on the four URE3 EMS domain accounts annually. These domain accounts were set up to serve all of URE3's CFE assets. Upon discovery, these CFE passwords were also changed.

The UREs initiated a review to determine if there were other accounts in the URE1 and URE3 EMS environments that had not had passwords changed annually. For the URE1 EMS environment, it was determined that a number of local administrator accounts for the CFE assets had not had passwords changed since their acquisition, which was prior to the date of mandatory compliance. These passwords were changed as they were discovered. For the URE3 EMS environment, it was determined that a number of local administrator accounts for the CFE assets had not had passwords changed annually, as well as the passwords for two application personal computers. Most had not been changed since prior to the date of mandatory compliance. These passwords were also changed as they were discovered.

During the course of mitigation of this violation, the UREs identified the need to file a TFE for the technical infeasibility of changing passwords on some accounts in use on EMS database servers. Additionally, through the mitigation efforts, MRO discovered that the UREs were relying solely on procedural controls for password changes on some accounts, without implementing technical controls as required by CIP-007-1 R5.

Additionally, SPP RE and WECC discovered issues with passwords on devices at Critical Asset substations during the Joint Compliance Audit. Specifically, the passwords on substation relays within the ESP did not meet the complexity requirements of CIP-007-1 R5.3. However, the issues were

mitigated through the submission of several TFEs, because the substation relays could not support the required password complexity rules.

MRO determined that the UREs had a violation of CIP-007-1 R5 for failing to require and use passwords subject to the complexity and change requirements of the standard.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The local administrator account on each CFE was not changed for a lengthy period. The CFE devices were the "front line" of the EMS, serving as the first line of communication that the EMS had with remote BPS facilities. While the UREs did not employ routable communications between Critical Asset substations and the EMS, they did use routable communications between two of the CFEs and some of the non-BPS substation facilities. The domain accounts that were originally identified and that could be used to access any of the CFE devices had not been changed in over a year. Further, a number of personnel with knowledge of these passwords left the employment of the UREs during the violation period.

However, the UREs configured firewalls between these two CFEs and those non-BPS facilities that limited the network traffic allowed from the remote terminal units into the CFEs. In addition, the UREs verified that no network connection has ever been initiated from these non-BPS facilities into these CFEs. Lastly, TFEs were appropriate for the EMS database issue, as the vendor did not support password changes for those accounts.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. train EMS staff on the CIP-007-3 R5.3.3 requirement;
2. place recurring reminders on the electronic calendars of EMS staff for changing the passwords in future years;
3. create recurring tracking items in the UREs' regulatory compliance database to provide a further level of notice/reminder/review and to ensure the password change is not missed in the future;
4. change passwords on all CFE domain and local administrator accounts; and
5. submit TFEs as necessary.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R7 (R7.1, R7.2) (MRO201100292)

URE1 submitted a Self-Report stating that it was in violation of CIP-007-1 R7. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

During an internal inventory of Cyber Assets within the ESP, URE1 and URE3 (collectively, the UREs) identified discrepancies between listed Cyber Assets and those deployed in the field. After further review, it was determined that certain substation CCAs decommissioned after a certain date had not been handled in a manner consistent with the UREs' substation change control and configuration management process.

During mitigation activities, the UREs determined that there were five instances of disposal or redeployment of substation CCAs subject to CIP-007 R7 (three for URE1 and two for URE3). Activities conducted for these changes did not follow the requirements of the UREs' substation change control and configuration management process.

MRO determined that the UREs had a violation of CIP-007-1 R7 for failing to implement their methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESPs.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The five devices consisted of three relays and two local control units. These devices were accessible only via dialup and did not communicate via routable protocol within the substation. Therefore, the information to be retrieved from these devices after their removal would have included only such things as protection system settings and device configuration, which would have presented a minimal risk to cybersecurity.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the pre-commissioning checklist;

3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement it using the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;
9. inform MRO of status of contacting the other utilities; and
10. execute additional action plan to augment the substation change control process and resolve any remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

Regional Entity's Basis for Penalty

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

1. MRO did not consider the UREs' compliance history as an aggravating factor in the penalty determination;
2. the UREs had an internal compliance program at the time of the violation which MRO considered a mitigating factor;
3. MRO awarded significant mitigating credit to the UREs for their commitment to the development, implementation, and continuous improvement of their corporate compliance program;

4. the UREs committed to retain an independent, third-party consultant to evaluate opportunities for enhanced CIP management controls, both under the current requirements and in preparation for the transition to CIP Version 5, at an estimated cost of $205,000;
5. the UREs self-reported several of the violations;
6. the UREs were cooperative throughout the compliance enforcement process;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. the violations of CIP-003-2 R5, CIP-004-2 R3, CIP-006-1 R1, CIP-006-3 R2, and CIP-007-1 R5 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
9. the remaining violations posed a minimal or moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

As noted above, MRO awarded significant mitigating credit to the UREs' commitment to continuous improvement in the area of CIP compliance. The UREs' efforts to improve their program include reorganizing teams to create groups to enhance security through CIP compliance, conducting regular reviews of CIP compliance issues, creating and working through various project plans to improve their CIP cybersecurity posture, adding personnel, and instituting a robust Risk-Based Assessment Methodology.

After consideration of the above factors, MRO determined that, in this instance, the penalty amount of one hundred and fifty thousand dollars ($150,000) 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**[5]

**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,[6] the NERC

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *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).

BOTCC reviewed the Settlement Agreement and supporting documentation on November 11, 2014 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.

In reaching this determination, the NERC BOTCC also considered the factors considered by MRO as listed above.

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

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

**Attachments to be Included as Part of this Notice of Penalty**

REDACTED FROM THIS PUBLIC VERSION

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

| | |
|---|---|
| Gerald W. Cauley<br>President and Chief Executive Officer<br>North American Electric Reliability Corporation<br>3353 Peachtree Road NE<br>Suite 600, North Tower<br>Atlanta, GA 30326<br>(404) 446-2560<br><br>Charles A. Berardesco*<br>Senior Vice President and General Counsel<br>North American Electric Reliability Corporation<br>1325 G Street N.W., Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>charles.berardesco@nerc.net | Sonia C. Mendonça*<br>Associate General Counsel and<br>Senior Director of Enforcement<br>North American Electric Reliability Corporation<br>1325 G Street N.W.<br>Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>sonia.mendonca@nerc.net<br><br>Edwin G. Kichline*<br>Senior Counsel and Associate Director,<br>Enforcement Processing<br>North American Electric Reliability Corporation<br>1325 G Street N.W.<br>Suite 600<br>Washington, DC 20005<br>(202) 400-3000<br>(202) 644-8099 – facsimile<br>edwin.kichline@nerc.net |

| | |
|---|---|
| Daniel P. Skaar*<br>President<br>Midwest Reliability Organization<br>380 St. Peter Street, Suite 800<br>Saint Paul, MN 55102<br>P: 651-855-1731<br>dp.skaar@midwestreliability.org<br><br>*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. | Sara E. Patrick*<br>Vice President of Regulatory Affairs and Enforcement<br>Midwest Reliability Organization<br>380 St. Peter Street, Suite 800<br>Saint Paul, MN 55102<br>P: 651-855-1708<br>se.patrick@midwestreliability.org |

**Conclusion**

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

Respectfully submitted,

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

*/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
Associate General Counsel and
Senior 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

cc: Unidentified Registered Entities
Midwest Reliability Organization

Attachments