Federal Energy Regulatory Commission
Washington, D.C. 20426

January 25, 2022

FOIA No. FY9-30 (RC11-6)
Fifty Fourth Determination Letter
(Release)

**VIA ELECTRONIC MAIL ONLY**
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This is a response to your correspondence received in January 2019, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated January 13, 2022, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC11-6, along with the names of fourteen (14) relevant UREs disclosed, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

**Identities of Other Remaining UREs Contained Within RC11-6.**

With respect to the remaining identities of UREs contained in RC11-6, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the

[1] 5 U.S.C. § 552 (2018).

[2] This docket involves multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the UREs for whom FERC initially determined that disclosure of identities may be appropriate.

Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC11-6 will not be disclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney T. Anthony Quinn by email at Tony.Quinn2@usdoj.gov, by phone at (202) 252-7558, or

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2022.01.25 12:49:15 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

Peter Sorenson, Esq.
Counsel for Mr. Mabee
petesorenson@gmail.com

James M. McGrane
Senior Counsel
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, D.C. 20005
James.McGrane@nerc.net

| Region | Name of Entity | NCR | Issue Tracking # | Standard | Req. | Description of Remediated Issue | Description of the Risk Assessment | Description and Status of Mitigation Activity |
|---|---|---|---|---|---|---|---|---|
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) | NCRXXXXX | FRCC200900250 | BAL-005-0.1b | R11 | The entity self-reported that it did not include the effects of ramp rate when calculating Area Control Error (ACE) and the Scheduled Interchange values were also not identical and agreed to by the affected BAs. | The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: (1) the mismatch was only between a 10 or 20 minute ramp rate in the Scheduled Interchange between affected BAs and there were no subsequent issues reported for Control Performance Standards (CPS1 and CPS2) for BAL-001-0a by the affected entities; (2) the only potential effect to the BPS has been a temporary increase in inadvertent energy during the ramp times; (3) in a sample of electronic tags (e-tags) the maximum amount of ramping was for 15 MW with the majority of e-tag changes being between 1 and 2 MW; and (4) the entity is exclusively a power importer and imports a relatively small amount of power. | The entity no longer approved or implemented any e-tags that do not specifically include the ramp start or stop duration times. In addition, the entity upgraded its Supervisory Control and Data Acquisition (SCADA) system to include ramp rates in the ACE equation. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) | NCRXXXXX | FRCC201000367 | FAC-009-1 | R1 | The entity self-reported that it had a Facility Ratings Methodology for its relay protective devices (per FAC-008-1); however, the Ratings Methodology had not been applied to those devices to determine the actual Ratings. | The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had been operating its equipment within manufacturer's specifications. | The entity revised and then applied the FAC-008-1 Methodology to its relay protective devices to determine Ratings. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) | NCRXXXXX | FRCC201000390 | FAC-001-0 | R1 | The entity self-reported that it had no facility connection requirements procedure from June 18, 2007 through September 17, 2007. | The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all applicable sub-requirements would have been discussed and negotiated during the engineering studies related to an interconnection. In addition no interconnections were made during the time period and the entity had a document for connections to its electric system in place though the document did not specifically address the BPS. | The entity created a facility connections requirements procedure. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) | NCRXXXXX | FRCC201000394 | FAC-008-1 | R1.3 | The entity self-reported that its evidence was insufficient to demonstrate that the entity had included in its Facility Ratings Methodology document:<br>(1) Ambient conditions for relay protective devices and terminal equipment, as required by R1.3.3.<br>(2) Operating conditions for transmission conductors, terminal equipment and protective relay devices, as required by R1.3.4.<br>(3) Other assumptions for transmission conductors, terminal equipment and protective relay devices, as required by R1.3.5. | The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had been operating its equipment within manufacturer's specifications. | The entity revised its FAC-008-1 documentation to include the missing R1.3 sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) | NCRXXXXX | FRCC201000404 | FAC-001-0 | R2 | The entity was found at a compliance audit that its facility connections requirements document was insufficient to demonstrate that the entity had:<br>(1) Procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible, as required by R2.1.2.<br>(2) Voltage level and MW and MVAR capacity or demand at point of connection, as required by R2.1.3. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all applicable sub-requirements would have been discussed and negotiated during the engineering studies related to an interconnection if there had been a request to interconnect. In addition no interconnections were made during the time period. | The entity revised its documentation to include the missing procedures for notification of new or modified facilities to others (those responsible for the reliability of the interconnected transmission systems) as soon as feasible and included MW and MVAR capacity demand at point of connection. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 1 (FRCC_URE1) New Smyrna Beach, Utilities Commission of | NCRXXXXX | FRCC201000339 | CIP-002-1 | R1 | The entity self-reported that the entity's risk-based assessment methodology as required by CIP-002-1 R1 was not in effect as of the date in which the entity was required to be in compliance. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity using its own risk-based assessment methodology, determined that it had no Critical Assets that could impact BPS reliability. In addition, the entity is relatively small. | The entity created a risk-based assessment methodology and Critical Asset list. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 2 (FRCC_URE2) | NCRXXXXX | FRCC200910003 | PRC-005-1 | R1 | The entity self-reported that its documents were insufficient to demonstrate that the Protection System maintenance and testing program for generation Protection Systems that affect the bulk power system (BPS) included a basis for protective relays, associated communication systems, DC control circuitry, and voltage and current sensing devices and station batteries.<br>There was insufficient evidence to demonstrate that the Protection System maintenance and testing program for generation Protection Systems that affect the BPS included an interval for the maintenance and testing of protective relays, voltage and sensing devices and station batteries.<br>The evidence was also insufficient to demonstrate that the Protection System maintenance and testing program for generation Protection Systems that affect the BPS included an interval for the maintenance and testing of DC control circuitry, associated communication systems.<br>There was insufficient evidence to demonstrate that the Protection System maintenance and testing program for generation Protection Systems that affect the BPS included a summary of maintenance and testing procedures for protective relays, DC control circuitry, voltage and sensing devices, station batteries and associated communications systems. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because the issue was discovered and self-reported prior to the June 18, 2007 effective date and mitigation began as early as March 2008 even though after a Spot Check, FRCC required the entity to perform additional mitigation activities. In addition, the entity is a very small generating facility. | The entity included all required items in its generation Protection System maintenance and testing program, including maintenance and testing intervals and their basis, as required by R1.1 and a summary of maintenance and testing procedures, as required by R1.2 for all its Protection System devices. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 2 (FRCC_URE2) | NCRXXXXX | FRCC200900303 | PRC-005-1 | R2 | The entity self-certified that it did not follow its generation Protection System maintenance and testing program. The entity could not provide documentation of its current transformer (CT) and potential transformer (PT) preventative maintenance for CTs and PTs associated with turbine generator 2 and for PTs associated with turbine generator 1, as specified in the entity's preventative maintenance program. This included 51 components out of 159 total Protection System devices. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the CTs and PTs output would have alarmed the control room if any issues occurred. In addition, the entity is a small generating facility. | (1) The entity performed required preventative maintenance for CTs and PTs in accordance with the procedures provided in its generator Protection System preventative maintenance program<br>(2) The entity updated its tracking matrix and reported compliance to FRCC.<br>Mitigation was completed and FRCC verified completion. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200700048 | COM-001-1 | R5 | The entity self-certified that it lacked sufficient evidence to demonstrate it had written operating instructions and procedures to enable continued operation of the system during the loss of telecommunication facilities at its control center and substations. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because in case of loss of telecommunications facilities, system operators are instructed by other company documents and procedures to utilize cellular phones to maintain communications. In addition, the entity is relatively small. | The entity revised the procedure to include instructions on continuing operation of the system during the loss of telecommunication facilities as specified in COM-001 R5. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200910002 | PER-002-0 | R3.4 | The entity self-reported that it lacked sufficient evidence to demonstrate that all of its training staff had instructional capabilities. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had instructors with sufficient operational capabilities in addition to at least one employee (though not all) with the required instructional capabilities. In addition, the entity is relatively small. | The entity revised its system operator training program to include only the trainer with proper training credentials. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900188 | EOP-001-0 | R3.3, 3.4 | The entity self-reported that it lacked sufficient evidence to demonstrate it had developed, maintained and implemented a set of plans for load shedding and system restoration. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not have a documented procedure, there is a load reduction schedule implemented in its SCADA system. The system operators had been instructed in its use and have the authority to restore the system and to shed load as needed to maintain Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs). In addition, the entity is relatively small. | The entity developed, maintained and implemented a set of plans for load shedding and system restoration. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900189 | EOP-001-0 | R4 | The entity self-reported that it lacked sufficient evidence to demonstrate it had a procedure for communication protocols to be used during emergencies. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not have documented communication protocols, FRCC believes that the entity's system operators understood, had tools and would have implemented the necessary communications required during an emergency due to requirements in other company documents. In addition, the entity is relatively small. | The entity developed, maintained and implemented a set of plans for mitigating operating emergencies. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900190 | EOP-001-0 | R5 | The entity self-reported that it did not have a documented emergency plan that included the applicable elements in Attachment 1 of EOP-001-0.<br><br>The entity lacked sufficient evidence to demonstrate it included one applicable element (as listed in Attachment 1 of EOP-001-0) in its emergency plan including (8) appeals to customers to use alternate fuels. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had all other applicable elements from Attachment 1 in its program and had no large industrial or commercial users. In addition, the entity is relatively small. | The entity created an emergency plan that incorporated all of the sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900192 | EOP-001-1 | R7.1, R7.3 | The entity self-reported that it had no procedure for communication protocols, as required by R7.1. The entity's current procedure provides evidence that the entity established and maintained reliable communications between interconnected systems. The entity's current procedure also has a procedure for communication protocols, as required by R7.3. The entity's evidence was insufficient to show to the time of the mitigation that the entity coordinated transmission maintenance schedules to maximize capacity. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not have documented communication protocols, FRCC believes that the entity's system operators understood, had tools and would have coordinated those tools and procedures in place due to requirements contained in other company documents. In addition, the entity is relatively small. | The entity updated its procedure for communication protocols to include all of the sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900195 | EOP-003-1 | R8 | The entity was found at a compliance audit to have insufficient evidence to demonstrate the entity had operator controlled manual load shedding plans to respond to real-time emergencies. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity's system operators were given the authority to shed load to respond to real time emergencies through other company documents. In addition, the entity is relatively small. | The entity created a load shed plan that incorporated all of the R8 sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900196 | EOP-005-1 | R1 | The entity was found at a compliance audit to not have a documented emergency plan that included the applicable elements in Attachment 1 of EOP-005-1.<br><br>The entity lacked sufficient evidence to demonstrate it included applicable elements (as listed in Attachment 1 of EOP-005-0) in its emergency plan (namely loss of communication power supplies). | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because FRCC believes that the entity's system operators understand and would have implemented the necessary communications required during an emergency due to the requirements contained in other company documents. In addition, the operators have multiple communication methods and would have responded to the loss utilizing an alternate communication path. In addition, the entity is relatively small. | The entity revised its emergency plan to incorporate loss of communication power supplies. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900199 | EOP-005-1 | R4 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that it had plans for control center loss of functionality. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not have a completely documented plan for control center loss of functionality, the entity did have a partial plan for use after April 29, 2008. In addition, the entity is relatively small. | The entity revised its contingency plan to include all of the missing sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900201 | EOP-008-0 | R1 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that it had plans for control center loss of functionality. The entity put in place a partial plan which met the requirements of the standard with the exception of subrequirements 1.5 and 1.6. These requirements state as follows: R1.5. The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.<br>R1.6. The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not have a completely documented plan for control center loss of functionality, the entity subsequently had a partial plan for use, which met subrequirements R1.1, R1.3, R1.4, R1.7 and R1.8 (R1.2 is not applicable to the entity). Even though the plan was missing a component for R1.5 and R1.6 the entity was conducting training on the plan and conducting the periodic tests to ensure viability of the plan. In addition, the entity is relatively small. | The entity revised its contingency plan to include all of the missing R1 sub-requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC200900202 | PRC-004-1 | R1 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that the entity developed and implemented a Corrective Action Plan to avoid future Misoperations. A relay misoperated due to its being wired incorrectly where two phases (the "C" and "B" phases) were swapped. It was determined that the misoperation occurred on the entity's end of a 138 kV tie line. The wiring problem was corrected and the entity completed a transmission disturbance analysis review report with initial findings and a conclusion, which resulted in the repair being made. The only item missing from the disturbance report were actions that the entity would take to avoid future Misoperations of a similar nature. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the entity did not address future avoidance of Misoperations, it did perform a Corrective Action Plan and checked all of the other relays in its system for miswired relays which could cause future Misoperations. In addition follow-up tests of system relays indicated that no other wiring issues existed of a similar nature to their relays. Finally, the entity is relatively small. | The entity tested other BPS relays on its system to determine if any other relays were wired incorrectly like the one that caused the event, and created a checklist to ensure correct testing procedures are utilized in the future. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 3 (FRCC_URE3) | NCRXXXXX | FRCC201100430 | TOP-003-0 | R1.2 | The entity self-reported that it did not follow the Reliability Coordinator (RC)'s outage reporting requirements to provide outage information daily to its RC, affected Balancing Authorities (BAs) and Transmission Operators (TOPs) for scheduled bulk transmission outages planned for the next day that may collectively cause or contribute to an Interconnection Reliability Operating Limit (IROL) or System Operating Limit (SOL) violation or a regional operating area limitation. The entity did not have any unscheduled outage. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the scheduled outage was not reported on the Florida Transaction Messaging System (FTMS) as required by the RC, it was listed in the current day and next day daily flow emails which were sent to the RC, BA and neighboring TOP. The RC stated that it did receive the outage information via e-mail and did include the outage in its daily study. In addition, the entity is relatively small. | The entity revised its procedures to notify the RC through FTMS in case of a planned outage in accordance with FRCC handbook requirements. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 4 (FRCC_URE4) | NCRXXXXX | FRCC200900253 | BAL-005-0.1b | R11 | The entity self-reported that it had approved electronic tags (e-tags) that did not include ramp start and/or stop times and did not include the effects of ramp rate when calculating Area Control Error (ACE). | The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br><br>(1) The mismatch was only between a 10 and a 20 minute ramp rate in the Scheduled Interchange between affected Balancing Authorities and there were no subsequent violations reported for Control Performance Standards (CPS1 and CPS2) for BAL-001-0a by the affected entities.<br>(2) The entity serves exclusively as a power importer and imports only a relatively small amount of power.<br>(3) The only potential effect to the BPS has been a temporary increase in inadvertent energy during the ramp times.<br>(4) In a sample of e-tags, the maximum amount of ramping was for 18 MW with the majority of e-tags changes being between 10 and 12 MW. | The entity stopped accepting blank e-tags and installed software which managed all tags, provided schedule information to the Automatic Generation Control (AGC) function and provided local storage of e-tags. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 4 (FRCC_URE4) | NCRXXXXX | FRCC200900333 | FAC-001-0 | R1 | The entity self-certified that it did not document, maintain and publish facility connections requirements. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all applicable sub-requirements would have been discussed and negotiated during the engineering studies related to any proposed interconnection. In addition, the entity is relatively small and there is limited BPS exposure for that portion of the BPS as the entity is only connected to one other Transmission Operator. | The entity developed the required facility connections requirements document and emailed it to the relevant entities and posted it to the entity's public website. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 4 (FRCC_URE4) | NCRXXXXX | FRCC200900318 | FAC-010-1 | R1 | The entity self-certified that it did not have a documented System Operating Limit (SOL) Methodology for use in developing SOLs within its Planning Authority Area. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity is relatively small and there is limited BPS exposure for that portion of the BPS as the entity is only directly connected to one other Transmission Operator (TOP) and its Ratings have been provided through the regional planning process to that TOP. | The entity developed a documented SOL Methodology which included: (a) being applicable for developing SOLs used in the planning horizon; (b) stating that SOLs shall not exceed associated Facility Ratings; and (c) including a description of how to identify the subset of SOLs that qualify as Interconnection Reliability Operating Limit (IROLs). The document was posted on the FRCC website and issued to affected entities. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 4 (FRCC_URE4) Homestead, City of (HST) | NCRXXXXX | FRCC201000352 | CIP-002-1 | R1 | The entity self-reported that its earliest risk-based assessment methodology, as required by CIP-002-1 R1, was not effective as of the date in which the entity was required to be in compliance and hence, the entity was in noncompliance with this Standard. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk-based assessment was not documented for only a period and when it was applied did not result in any Critical Assets. In addition, the entity is relatively small. | The entity completed a risk-based assessment methodology and no Critical Asset were identified. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 5 (FRCC_URE5) | NCRXXXXX | FRCC201000343 | PRC-005-1 | R1 | The entity was found during a Spot Check to have insufficient evidence that the entity had a Protection System maintenance and testing program that had a basis for intervals for associated communication systems, voltage and current sensing devices and DC control circuitry; and the documentation was insufficient evidence that the entity had a Protections System maintenance and testing program with maintenance and testing intervals for voltage and current sensing devices. | This issue posed a minimal risk and did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating and testing its equipment within manufacturer's recommendations and test records were reviewed as part of the Spot Check and were found to be within interval. | The entity performed Protection System maintenance and testing document revisions. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 5 (FRCC_URE5) | NCRXXXXX | FRCC201000399 | FAC-008-1 | R1 | The entity was found at a compliance audit to not include the complete scope of equipment for relay protective devices, terminal equipment (CTs/PTs), and series and shunt compensation devices, as required by R1.2.1, as well as ambient conditions, operating limitations and other assumptions for scope of equipment such as bus ducts, generator transformers, and circuit breakers, as required by R1.3.3 - R1.3.5, in its generation Facility Ratings Methodology. The entity was applying with its transmission Facility Ratings Methodology. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating its equipment within manufacturer's specifications and the Ratings did not change after completion of the entity's mitigation plan. | The entity developed a Facility Ratings Methodology that included all equipment and conditions and then applied the Methodology to all generation Facilities to recalculate the generation Facility Ratings to ensure accuracy. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 5 (FRCC_URE5) | NCRXXXXX | FRCC201000400 | PRC-005-1 | R2 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that the entity complied with its transmission Protection System testing and maintenance intervals, as required by R2.1. Specifically, quarterly battery testing was delayed by 12 days for one transmission substation due to broken test equipment. This included one battery bank out of 251 total Protection System devices. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because though the entity did not meet its required testing intervals for one of its quarterly battery tests, the entity did meet its testing intervals for monthly, annual and all other quarterly battery tests. | The entity performed testing prior to the mitigation plan; effectively mitigating the violation. In the mitigation plan, the entity stated it reemphasized the importance of testing to its substation maintenance group and revised its Protection System maintenance and testing program to add flexibility for reasonable and/or acceptable delays to testing that may occur. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 5 (FRCC_URE5) | NCRXXXXX | FRCC201000401 | PRC-005-1 | R2 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that the entity complied with its testing and maintenance intervals, as required by R2.1. The entity's power plant battery banks annual load testing was delayed. This included one battery bank out of 251 total Protection System devices. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because though the entity did not meet its required testing intervals for one of its annual battery tests, the entity did meet its testing intervals for monthly and all quarterly battery tests and annual test delay was for relatively short period (31 days). | The entity performed testing prior to the mitigation plan, effectively mitigating the violation. In the mitigation plan, the entity stated it reemphasized the importance of testing to its generation instrumentation and electrical group and revised its Protection System maintenance and testing program to add flexibility for reasonable and/or acceptable delays to testing that may occur. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 6 (FRCC_URE6) | NCRXXXXX | FRCC201000358 | FAC-008-1 | R1, R1.2, R1.3 | The entity was found at a compliance audit to have insufficient evidence to demonstrate that its Facility Rating Methodology addressed the following: The scope of equipment did not address relay protective devices and terminal equipment, as required by R1.2.1. The scope of Ratings did not include both Normal and Emergency Ratings for relay protective devices, as required by R1.2.2.<br>In addition, the Facility Ratings Methodology did not address the following: Equipment manufacturers for relay protective devices and terminal equipment, as required by R1.3.1;<br>design criteria, as required by R1.3.2; ambient conditions, as required by R1.3.3; operating limitations, as required by R1.3.4; and other assumptions for the following: generators, transmission conductors, transformers, relay protective devices and terminal equipment, as required by R1.3.5. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the Ratings were developed during the design of the Facility and the final commissioning of the plant. Also the entity was operating its Facility as per the manufacturer's specifications. In a study conducted upon commissioning, it was determined that the turbines were the most limiting equipment and the entity's equipment and Ratings have not changed since commissioning. | The entity reviewed and confirmed its previous Facility Rating Methodology. It established and documented a modified nameplate listing and/or reference drawing Ratings cataloging the methodology of major BPS equipment in the entity's FAC-008-1 document. |
| Florida Reliability Coordinating Council, Inc. (FRCC) | Unidentified Registered Entity 7 (FRCC_URE7) | NCRXXXXX | FRCC200900294 | PRC-008-0 | R1 | The entity self-reported that it did not have a maintenance and testing program to address its UFLS relays. | This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity has attested it had performed some maintenance and testing, but had not created the documentation. In addition, the entity is very small. | The entity created a maintenance and testing document for its UFLS relays. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 1 (MRO_URE1) Wisconsin Public Service Corporation (WPS) | NCRXXXXX | MRO201100309 | CIP-006-1 | R1 | The entity self-reported noncompliance with CIP-006-1 R1 because it discovered that its physical security plan was not approved by a senior manager or delegate. The violation was discovered during an internal audit performed by a third-party industry expert. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue related to the failure to obtain the required signature and did not change the development or implementation of the physical security plan. | The entity performed the following actions to mitigate the issue: (1) revised its CIP leadership designation procedure and removed chief security officer involvement in designating the senior leader; (2) the senior security specialist was advised of the errors and the proper method of delegating authority from the senior manager to another individual, and the proper method of documenting review and approval of the NERC CIP physical security plan; (3) the physical security plan was modified to explicitly state who can approve the plan and that the approval has to be documented; (4) a formal delegation form for the chief security officer was completed evidencing the delegation of authority to review and approve the physical security plan; (5) the chief security officer reviewed and approved the NERC CIP physical security plan; (6) the physical security plan was modified to explicitly state that all changes require the review of the senior manager or his delegate; and (7) a review of all CIP requirements were performed to identify whether other areas require review or approval of the senior manager or delegate. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 2 (MRO_URE2) | NCRXXXXX | MRO201000238 | CIP-004-1 | R2 | The entity self-reported noncompliance with CIP-004-1 R2 because two contractors were not added to the authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) access list. The entity failed to record the access approval on the list. As a result of not being added to the access list, two contractors did not have cyber security training within the required timeframe. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the two CCAs that were accessed were later classified as non-critical Cyber Assets. They are not essential to the operation of the generating unit and have been moved from the Electronic Security Perimeter. | The entity reclassified the CCAs as non-critical Cyber Assets. Additionally, personnel involved in granting access have been reminded of the processes required for authorized cyber or authorized unescorted physical access. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 2 (MRO_URE2) | NCRXXXXX | MRO201000239 | CIP-004-1 | R3 | The entity self-reported noncompliance with CIP-004-1 R3 because one contractor was provided access to Critical Cyber Assets (CCAs) before the compliance date. However, this contractor was not added to the access list during the substantial compliant period for the Cyber Assets. As a consequence of not being added to the access list, this contractor did not have a personnel risk assessment (PRA) conducted pursuant to the entity's PRA program prior to such personnel being granted such access. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the CCA was later determined to be non-critical and was later removed from the Electronic Security Perimeter. | The entity revoked access to the CCAs for the individual. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 2 (MRO_URE2) | NCRXXXXX | MRO201000240 | CIP-004-1 | R4 | The entity self-reported noncompliance with CIP-004-1 R4 because three contractors were not added to the authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) access list and two contractors were not removed from the access list as required by CIP-004-1 R4. Three contractors accessed three personal computers at 2 of the entity's generating stations. The contractors were from three different companies. Additionally, two janitors from one janitorial contractor were not removed from the list of personnel with authorized unescorted physical access within seven calendar days of their not-for-cause termination. Both janitors were terminated during the substantially compliant period but were not deleted from the list. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because two of the CCAs that were accessed were later classified as non-critical Cyber Assets. They are not essential to the operation of the generating unit and have been moved from the Electronic Security Perimeter. Additionally, one CCA was accessed with view only privileges. The two janitors did not have access to the CCAs. They were just not removed from the list. | The entity reclassified the CCAs as non-critical Cyber Assets. The entity removed the janitors from the access list. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 3 (MRO_URE3) | NCRXXXXX | MRO201000241 | CIP-004-1 | R4.1 | The entity self-reported noncompliance with CIP-004-1 R4 because its authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) access lists were not updated within 7 calendar days of the granting of access for 3 of 546 (less than 1%) individuals. Specifically, two access requests were processed out of order, and therefore, were not routed through the appropriate workflow. The other access was due to an oversight in documentation. The administrator that configured the access was configuring appropriate access per verbal approval for access, but failed to document the approval. As a result, the list of authorized personnel was not updated within 7 calendar days of a change in access rights of the personnel. One individual retained access for 18 days, another individual retained access for 52 days, another individual retained access for 5 days following the change in business need. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because all of the individuals had personnel risk assessments and cyber security training. Additionally, logs from the card reader system and user access logs demonstrate that access was not used for each individual. | At the point of discovery, the appropriate requests were submitted and completed correctly by personnel, removing access the same day. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 4 (MRO_URE4) | NCRXXXXX | MRO201000243 | CIP-004-1 | R4.1 | The entity self-reported noncompliance with CIP-004-1 R4 because its authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) access lists were not updated within 7 calendar days of the granting of access for 3 of 546 (less than 1%) individuals. The removal tasks were routed appropriately but were processed incorrectly. Specifically, removal tickets were submitted in the access management tool, the work tickets were routed appropriately, but, at the last step, the guard staff failed to go into the badging server and remove the access from the badge. Therefore, the access list was updated, but the access remained on the actual badges. As a result, personnel were removed from the list of authorized personnel without actual revocation of access within the card access system, causing retention of access in excess of 7 calendar days. One individual retained access for 88 days following the change in business need, another individual retained access for 189 days following the change in business need, and another individual retained access for 63 days following the change in business need. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the access removals were related to job changes, rather than for cause terminations. Additionally, logs from the card reader system and user access logs demonstrate that access was not used for each individual. | At the point of discovery, the appropriate requests were submitted and completed correctly by personnel, removing access the same day. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 5 (MRO_URE5) | NCRXXXXX | MRO201100254 | CIP-009-2 | R1 | The entity self-reported noncompliance with CIP-009-2 R1 because it did not have recovery plans for assets declared as Critical Cyber Assets. The assets were misclassified as Critical Cyber Assets in early versions of the entity's risk-based assessment methodology (RBAM). The entity's early methodology was overly broad and declared all Cyber Assets within the entity's Electronic Security Perimeters (ESPs) as Critical Cyber Assets. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the misclassified Cyber Assets in question reside within the entity's Physical Security Perimeters and ESPs and were protected by the existing security controls implemented by the entity. The entity has continued to refine its RBAM and assessment of assets that are critical to the operation of its Critical Assets. Additionally, mock audits and assessments brought this issue to light and thus, exemplify a strong culture of compliance at the entity. | The entity has mitigated the issue by correctly identifying these assets as Cyber Assets and in some cases has moved the devices outside ESPs where appropriate. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 5 (MRO_URE5) | NCRXXXXX | MRO201100257 | CIP-005-1 | R1.4, R1.6 | During a Spot Check, MRO determined that the entity failed to identify, protect, and document all noncritical Cyber Assets located within the Electronic Security Perimeter (ESP). MRO identified one noncritical Cyber Asset device (intermediate anti-virus server) that was moved "in and out" of the ESP every time the entity needed to update anti-virus signatures. Additionally, the entity failed to document another noncritical Cyber Asset device (network switch) which served as an access point to the ESP. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the intermediate anti-virus server was configured as a hardened single purpose device. Additionally, although it was not identified, the network switch was being protected by the entity's IT policy consistent with CIP-005. | The intermediate anti-virus server was relocated outside of the ESP. Additionally, the entity revised its anti-virus signature update process to eliminate the need to re-introduce the intermediate anti-virus server into the ESP each time the anti-virus signatures on the CCAs needed to be updated. The network switch was added to the entity's Cyber Asset inventory as a non-critical Cyber Asset residing within an ESP. IT then reviewed the protection being afforded to the network switch and confirmed it was being protected pursuant to the requirements of CIP-005. To confirm all Cyber Assets associated with Critical Assets were inventoried and properly classified, the entity decided to re-inventory its Cyber Assets. The inventory included a physical identification of the Cyber Assets followed by an electronic ping sweep of the Cyber Assets residing within the ESP. As a result of this process, and with the clearer understanding of the classification requirements gained through the evaluation of this finding, a similar network switch used to connect non-critical Cyber Assets within the ESP was identified and added to the entity's inventory of non-critical Cyber Assets. Unlike the first network switch, this switch was located within a Physical Security Perimeter. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 5 (MRO_URE5) | NCRXXXXX | MRO201100259 | CIP-006-1 | R1.1 | During a Spot Check, MRO determined that the entity failed to locate all Cyber Assets in a defined Electronic Security Perimeter (ESP) within an identified Physical Security Perimeter (PSP) and failed to incorporate a completely enclosed six-wall border for a PSP in its Physical Security Plan. MRO discovered an opening above the ceiling tiles in the breezeway connecting the control center and administration buildings. The opening allowed passage from the breezeway into the control center's designated PSP, bypassing access controls. Although the unprotected opening in the PSP boundary provided the ability to bypass access control mechanisms, access to any Critical Cyber Assets within the PSP requires clearance of additional access controls. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the entity's facility is protected against unauthorized access by three levels of physical security, and also includes video surveillance, and two levels of credential check-points. Additionally, although the unprotected opening in the PSP boundary provided the ability to bypass access control mechanisms, access to any Critical Cyber Assets within the PSP requires clearance of additional access controls. | During the spot check, MRO verified that the entity secured the opening with wire mesh, therefore restoring the six-wall border. MRO took photographs of the opening both before and after mitigation. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 5 (MRO_URE5) | NCRXXXXX | MRO201100331 | CIP-006-3c | R7 | The entity's corporate security on-call personnel were notified by the entity's security system contractor of a trouble alarm on the access control system. The support team was called in to review the system and locate the source of the alarm. The team first confirmed that the access control and logging system was operating properly at all the Physical Security Perimeter (PSP) access points. They then checked the system logs for any evidence of an attack or cyber intrusion following the appropriate procedure. No such evidence was found, and the incident response evaluation was documented. The team determined that the problem was associated with the nightly file backup process. The system logs indicated the nightly backup did not run completely. The team proceeded to restore following the change control, restoration, and testing procedures. The problem resurfaced on two more occasions. While the physical access system continued to provide the required access control and logging functionality, it was clear the system had a persistent technical problem. After the third incident, the team conducted a thorough analysis of all the services and discovered that the problem was a conflict between a replication application and the entity's automatic backup recovery system. Moreover, the in-depth analysis of the failures indicated that the data restoration process was actually corrupting the data while it was being restored. The entity self-reported noncompliance with CIP-006-3c R7 because an issue with its system led to corruption of physical access logs for its designated PSPs. Through recovery of corrupted log files and review of video surveillance recordings, all but five (5) hours of a 75-hour gap could be reconstructed. Therefore, the entity failed to retain physical access logs for at least ninety calendar days as required by CIP-006-3c R7. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because during the time logging did not function properly, the access controls were fully functional, and the five-hour gap was limited to two access points. Additionally, the gap in available logs spanned the time period of 12:03 pm to 5:27 pm CST. | The entity recovered all but five hours of the 75 hours of corrupted log files. Additionally, the entity reconfigured the system to preclude any subsequent data loss. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 6 (MRO_URE6) Basin Electric Power Cooperative (BEPC) [member is Northwest Iowa Power Cooperative (NIPCO)] | NCRXXXXX | MRO201000233 | CIP-001-1 | R1 | During a regularly scheduled compliance audit, MRO determined that the entity and one of its members failed to have a sabotage reporting procedure with procedures for the recognition of sabotage. | MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the procedure failed to provide instructions for identifying sabotage events, the employees were aware of the existence of the procedure and the issues involved in sabotage. Furthermore, the employees of the entity's member reported all potential or suspected incidents regardless of cause. Additionally, as part of the entity's risk-based assessment methodology to identify Critical Assets (CIP-002-3), no Critical Assets have been identified that are owned, operated, or maintained by the entity's member. | The entity's member adopted and trained its operating personnel on the entity's sabotage reporting procedure which included how to recognize and make operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 6 (MRO_URE6) | NCRXXXXX | MRO201000234 | FAC-003-1 | R1.3, R1.5 | During a regularly scheduled compliance audit, MRO determined that the entity and one of its members failed to (1) document the qualifications and training required for the design and implementation of the transmission vegetation management program (TVMP), as required by R1.3; and (2) document procedures for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage, as required by R1.5. | MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity and its member failed to document a procedure for the imminent communication of vegetation conditions that present an imminent threat of a line outage, their transmission lines are in a region of the U.S. that often experiences long growing times. Additionally, the entity's member has a TVMP which contains procedures for periodic ground inspections, not to exceed two years. | The entity revised its TVMP to include a documented procedure for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage and also revised its TVMP to incorporate the qualifications and training required for personnel responsible for the design and implementation of the TVMP. The entity's member revised its TVMP to include a documented procedure for the immediate communication of vegetation conditions that present an imminent threat of a transmission line outage. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 7 (MRO_URE7) | NCRXXXXX | MRO201000166 | PRC-008-0 | R2 | The entity self-reported that it failed to fully implement its UFLS maintenance and testing program. Upon receiving the entity's Self-Report, MRO requested a full inventory of the entity's UFLS equipment and maintenance and testing records. The entity has a total of 68 UFLS devices subject to PRC-008-0 R2. Of the 68 devices, 10 devices, or approximately 15%, did not have evidence of testing as required by PRC-008-0 R2. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the entity's identified UFLS equipment could only have had an 80 MW impact for load shed. Additionally, upon completing the required maintenance and testing, the entity's UFLS equipment performed as expected. | The entity took the following actions to mitigate the issue: (1) performed a complete inventory of each UFLS device or element and identified all deficiencies; (2) developed a "catch-up" maintenance and testing plan and schedule in order to correct the deficiencies; (3) trained its technicians regarding revisions to the transmission protection maintenance and testing program; (4) trained its technicians regarding "catch-up" testing; (5) notified personnel regarding revisions to its UFLS Protection System maintenance and testing program; (6) notified personnel in the "catch-up" maintenance and testing procedures; (7) completed the required "catch-up" maintenance and testing procedures. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 8 (MRO_URE8) | NCRXXXXX | MRO201100320 | PRC-005-1 | R1.1, R1.2 | During a regularly scheduled compliance audit, MRO determined that the entity failed to provide evidence of a Protection System maintenance and testing program (Program) for current and voltage sensing devices. The entity's Program addressed commission testing of current and voltage sensing devices, however once installed, the entity did not have maintenance and testing intervals and their basis or other test schedule for current and voltage sensing devices documented in its procedures. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because although the entity did not have current and voltage sensing devices documented within its Program, the entity was continuously monitoring its current and voltage sensing devices through the SCADA. | The entity revised its Program to include current and voltage sensing devices and their maintenance and testing intervals and their basis. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 8 (MRO_URE8) | NCRXXXXX | MRO201000170 | PRC-005-1 | R2.1, R2.2 | The entity self-reported noncompliance with PRC-005-1 R2 because during an internal review, the entity discovered that it was not meeting its testing intervals as required in its Protection System maintenance and testing program (Program). Specifically, station battery voltage measurements were not conducted every month as required in its Program. The Program document was written referencing a practice and form that has not been in effect since 2003. Prior to 2003, the entity was measuring the battery voltage on a monthly basis, but as of 2003, it has been the entity's practice to take measurements every other month. Additionally, the entity determined that battery hydrometer readings were not being conducted as required by the defined interval in the Program. Prior to 2003, the entity's practice was to conduct hydrometer tests twice per year. The entity's transmission maintenance department performed the hydrometer tests in both January and July. This test interval was changed in 2003. After 2003 the transmission maintenance department was to perform only the hydrometer tests in July, while the electrical maintenance personnel would perform the test in January. In this transition there was confusion as to who was to perform the July hydrometer tests. This confusion caused a lack of testing to be performed in 2009. Therefore, the entity was not compliant with its documented Program. Upon receiving the Self-Report, MRO requested that the entity perform a full inventory of its Protection System maintenance and testing records. In response, the entity reported that it has 1,314 Protection System devices subject to PRC-005-1 R2. Of the 1,314 devices, 20 devices lacked evidence of maintenance and testing records in accordance with its documented Program, or approximately 1.5%. The entity has 20 station batteries subject to PRC-005-1 R2. Each of the 20 batteries 100 kV and above did not meet the testing interval as required in the entity's Program. However, the entity's practice for measuring battery voltage is more stringent than the recommended timeframe in IEEE Standard 450. IEEE Standard 450 recommends measuring the individual cell voltage of a battery at least once per quarter. The entity provided evidence showing that 13 batteries met the IEEE Standard. Therefore, the entity was compliant with the IEEE voltage measurement Standard for 68% of its batteries. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity provided evidence of maintenance and testing according to the defined intervals for 98.5% of its Protection System devices. Additionally, the entity's practice for measuring individual cell voltage is more stringent than the recommended timeframe in IEEE Standard 450. IEEE Standard 450 recommends measuring the individual cell voltage of a battery at least once per quarter. The entity met this Standard for 68% of its station batteries. Therefore, the entity met the IEEE cell voltage Standard for the majority of its station batteries. The entity also monitors its station battery voltage continuously at the plant control room. Additionally, IEEE Standard 450 recommends measuring the specific gravity of each cell at least once per year. The entity's procedure for measuring specific gravity twice annually is more stringent than what is recommended by the IEEE Standard. The entity measured the specific gravity for all of its batteries within the IEEE Standard interval. Finally, there have been no battery system trouble alarms in the substations the entity owns and maintains that are 100 kV and above. Therefore, MRO determined that this issue posed a minimal risk to the BPS. | The entity has taken the following steps to mitigate the issue: (1) the entity's Program document was revised to coincide with the entity's established practice of testing transmission substation batteries; (2) the battery test report forms used to document battery maintenance and testing results were revised to include a better explanation of procedures and timelines and the new battery test report forms were distributed to all individuals involved in testing; (3) education of entity personnel conducting battery maintenance and testing took place to coincide with regularly scheduled safety meetings, and this training reviewed the entity's present procedure and practice of battery maintenance and reviewed the revised battery test report forms; (4) an internal review of testing notification procedures will take place at least once a year. The entity may consider a change in notification procedures and review of test reports to aid in an awareness of scheduled maintenance; (5) all substations had documented test results for the bi-monthly battery cell voltage test; and (6) all substations had documented test results for the hydrometer tests. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 9 (MRO_URE9) | NCRXXXXX | MRO201000208 | PRC-005-1 | R1.1; R1.2 | The entity self-reported noncompliance with PRC-005-1 R1 because a previous version of its transmission Protection System maintenance and testing program failed to document the interval, basis and summary of maintenance and testing procedures for certain Protection System devices. The entity reported that it did not have a documented Protection System maintenance and testing program, when it created a reference document stating that it contracts testing of relays to a third party. The entity then created a program document which addressed the maintenance and testing intervals and basis for Protection System relays. The entity implemented its protective relays preventative maintenance test schedules and procedures which included a summary of maintenance and testing procedures for relays. The entity's transmission and generation Protection System maintenance and testing program document was revised to include testing intervals and their basis for station batteries, current and voltage sensing devices, DC control circuitry, and associated communication devices. The entity's Protection Systems preventative maintenance test schedules and procedures were revised to include a summary of maintenance and testing procedures for associated communication devices, DC control circuitry, current and voltage sensing devices, and station batteries. Upon reviewing these documents, MRO determined that the entity failed to have a transmission Protection System maintenance and testing program that identified the maintenance and testing intervals and their basis, and a summary of maintenance and testing procedures for all Protection System devices as required by PRC-005-1 R1. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had a Protection System maintenance and testing program at the time it submitted the Self-Report. Furthermore, the entity maintained and tested all of its protective relays, monitors the DC control circuitry to the circuit breakers on a continuous basis via the SCADA system, and performs visual inspections on its exposed current transformers. The entity did not have any internal generation. All power was imported and load serving. Therefore, MRO determined that this violation posed minimal risk to BPS reliability. | The entity sold the majority of its transmission system and the majority of the transmission Protection System elements to a third party. Both the entity and the third party worked together to complete the following: (1) revised policies, guidelines and procedures and preventative maintenance test schedules and procedures to include interval, basis, and summary for the associated communication systems, DC circuitry, and instrument transformers associated with the transmission Protection Systems; (2) revised its procedures to include basis and summary for the protective relays associated with the transmission Protection Systems; and (3) obtained management approval for the new procedures. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 9 (MRO_URE9) | NCRXXXXX | MRO201000209 | PRC-005-1 | R2.1 | The entity self-reported noncompliance with PRC-005-1 R2 because it did not have evidence of maintenance and testing for its instrument transformers. Upon receiving the Self-Report, MRO requested an inventory of maintenance and testing records for all of the entity's Protection System devices subject to PRC-005-1 R2. The entity reported that it had 151 Protection System devices subject to PRC-005-1 R2. Of the 151 devices, the entity failed to provide maintenance and testing records for 95 of the devices, or approximately 63%, including 74 DC control circuits, 5 potential transformers (PTs), 14 current transformers (CTs) and 2 capacitance coupled voltage transformers (CCVTs). Therefore, MRO determined that the entity failed to provide evidence of maintenance and testing records for its transmission Protection System devices as required by PRC-005-1 R2.1. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity maintained and tested all of its protective relays, and although the entity did not record the test results, the entity monitors the DC control circuitry to the circuit breakers on a continuous basis via the SCADA system. The circuit breakers have two trip coils monitored by indicating lights. The entity reported that the indicating lights are checked on a weekly basis, although the inspections are not documented. The entity also reported that visual inspections are conducted on the exposed CTs and voltage transformers. The exposed CT outputs are continuously monitored by the SCADA system. The failure of associated communication devices and/or DC control circuitry would have been detected in near real time and corrective action would have been implemented. The entity did not have any internal generation. All power was imported and load serving. Therefore, for these reasons, MRO determined that this violation posed minimal risk to BPS reliability. | The entity sold the majority of its transmission system and the majority of the transmission Protection System elements to a third party. Both the entity and the third party worked together to complete the following: 1. for those transmission assets which the third party purchased from the entity, the third party determined a scope of work and prepared a work schedule for completing activities necessary to cause the acquired transmission assets to meet the requirements of that party's PRC-005 program document; 2. for those transmission assets which the third party has purchased from the entity, the third party completed work actions required to assure that the transmission assets conform to the testing and maintenance activities and intervals required by the third party's PRC-005 program document; 4. the third party submitted a report of the testing and maintenance results to the entity summarizing that appropriate actions have been completed and records assembled which demonstrated that the acquired transmission assets have been brought into conformance with the requirements of the third party's PRC-005 program document. The entity took the following corrective measures for the remaining transmission Protection System assets on the entity's distribution system: (1) reviewed all transmission Protective Systems remaining in place at the entity, determined transmission Protection System elements, and developed an updated master asset list; (2) utilizing the master asset list, developed a spreadsheet listing previous and next test dates; (3) tested applicable instrument transformers and DC circuitry; and (4) reviewed and approved maintenance and testing reports. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 10 (MRO_URE10) | NCRXXXXX | MRO201000187 | PRC-005-1 | R2.1, R2.2 | During a regularly scheduled compliance audit conducted by MRO, MRO determined that the entity failed to provide evidence that its station batteries were maintained and tested within the intervals defined in its transmission Protection System maintenance and testing program. Specifically, the entity was not able to provide evidence of weekly pilot cell voltage and specific gravity readings or the annual cell voltage, cell impedance or strap resistance readings for its station batteries. The entity explained that it discovered that the service crews were not aware of the battery maintenance and testing requirements. The entity reported that it has 97 Protection System devices subject to PRC-005-1 R2. Of the 97 devices, the entity failed to provide evidence of maintenance and testing for 14 devices, or approximately 14%. Specifically, the entity failed to provide evidence of maintenance and testing for 4 Protection System relays and 10 station batteries. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was performing more rigorous testing than required by the *NERC Protection System Maintenance Technical Reference Guide* (Guide). The Guide requires monthly tests, whereas the entity's Protection System maintenance and testing program required weekly tests. | The entity has performed the following actions to mitigate the issue: (1) performed an inventory of transmission protection equipment maintenance and testing records; and (2) completed all maintenance and testing of equipment that was identified during the inventory. Additionally, the entity reviewed its maintenance and testing policy and has adjusted the testing of the station batteries. The weekly test of the pilot cell voltage and specific gravity has been changed to a monthly test, and the entity is also recording the temperature of the pilot cell. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 10 (MRO_URE10) | NCRXXXXX | MRO201000188 | PRC-008-0 | R1 | During a regularly scheduled compliance audit conducted by MRO (Audit), MRO determined that the entity failed to identify all UFLS equipment, including station batteries, DC control circuitry, and frequency sensing devices in its UFLS equipment maintenance and testing program. During the Audit, MRO requested a copy of the entity's UFLS equipment maintenance and testing program. In response, the entity stated that its UFLS equipment is included in its policy for maintenance and testing of transmission protection equipment. However, this document did not identify UFLS equipment. Additionally, the entity also provided UFLS relay settings. Upon reviewing the document, MRO determined that the document was only specific to UFLS relays and failed to identify UFLS station batteries, DC control circuitry, and frequency sensing devices. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity only has two interconnection points. Furthermore, the entity will only shed 23 MW of UFLS load, therefore, a failure of any part of its UFLS program will have a minimal impact to the BPS. | The entity performed the following actions to mitigate the issue: (1) reviewed and updated its policy for maintenance and testing of transmission protection equipment, and made revisions to identify necessary UFLS equipment; and (2) revised its transmission protection equipment maintenance and testing lists to include additional UFLS equipment and testing schedules. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 10 (MRO_URE10) | NCRXXXXX | MRO201000189 | PRC-008-0 | R2 | During a regularly scheduled compliance audit conducted by MRO, MRO determined that the entity, was not able to provide maintenance and testing records of station batteries associated with its UFLS program. The entity provided the past maintenance and testing dates and the most recent UFLS relay maintenance and testing records. Specifically, the entity was not able to provide evidence of weekly pilot cell voltage and specific gravity readings or the annual cell voltage, cell impedance or strap resistance testing of its station batteries used in its UFLS program. The entity has 21 UFLS devices subject to PRC-008-0 R2. Of the 21 devices, the entity failed to provide evidence of maintenance and testing for 2 devices, or approximately 9.5%. Specifically, the entity failed to provide evidence of maintenance and testing for 2 station batteries. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity only has two interconnection points. Furthermore, because the entity will only shed 23 MW of UFLS load, a failure of any part of its UFLS program will have a minimal impact to the BPS. | The entity performed the following actions to mitigate the issue: (1) completed inventory of transmission protection equipment; (2) completed MRO questionnaire and identified all equipment that is part of the issue; and (3) completed all maintenance and testing of equipment that is out of the testing cycle. Additionally, the entity reviewed its maintenance and testing policy and has adjusted the testing of the station batteries. The weekly test of the pilot cell voltage and specific gravity has been changed to a monthly test, and the entity is recording the temperature of the pilot cell. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 11 (MRO_URE11) | NCRXXXXX | MRO200900139 | PRC-005-1 | R2.1 | The entity self-reported noncompliance with PRC-005-1 R2 because it did not have evidence that all required Protection System devices had been maintained and tested according to the intervals defined in its Protection System testing and maintenance procedure (Procedure), as required by R2.1. In response to the Self-Report, MRO requested that the entity perform a full inventory of its devices in order to determine whether there were any other missing records of maintenance and testing. Upon performing the review, the entity reported that within its generation Protection System, 68 relays had not been tested according to the defined interval, 1 battery lacked evidence of semi-annual testing, 51 voltage and current sensing devices had not been visually inspected according to the defined 3-year interval, and an additional 16 voltage and current sensing devices did not undergo annual testing. Additionally, the entity reported that within its transmission Protection System, 22 relays had not been tested according to the defined 72-month interval and 44 batteries had not been tested according to the defined testing interval. The entity has approximately 9,367 Protection System devices subject to compliance with PRC-005-1 R2 and was unable to provide evidence that approximately 2.2% of the devices were tested and maintained according to defined intervals. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because the entity provided evidence that it tested and maintained the overwhelming majority of its devices within its defined intervals. Additionally, although the entity failed to test 2.2% of its Protection System devices within its defined intervals, approximately 69% of those devices were tested within the *NERC Protection System Maintenance Technical Reference Guide* recommended intervals. Further, the entity quickly recognized and acknowledged the importance of correcting this issue and maintaining and testing its Protection System devices. Additionally, subsequent testing evidenced that the devices would have performed as anticipated. Therefore, MRO determined that this violation did not pose a serious or substantial risk to the BPS. | The entity performed the following actions: (1) performed a full inventory of its Protection System maintenance and testing records to determine whether any were missing; (2) performed all maintenance and testing on any devices missing maintenance and testing records; and (3) reviewed and revised its Procedures for generation and transmission Protection Systems in order to consolidate procedures. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 11 (MRO_URE11) | NCRXXXXX | MRO201000206 | PRC-005-1 | R1.1, R1.2 | The entity self-reported noncompliance with PRC-005-1 R1 because previous versions of its generation Protection System maintenance and testing programs failed to summarize its maintenance and testing procedures, and identify all applicable voltage and current sensing device equipment. The entity has seven generating plants. Each generating plant has its own Protection System maintenance and testing program. The entity reported that two of its generating plants did not have Protection System program documents which summarized the maintenance and testing procedures and identified the voltage and current sensing devices equipment. The entity also reported that the other five generation Protection System maintenance and testing programs failed to include summaries of the maintenance and testing procedures. Therefore, the entity failed to satisfy the requirements set forth in PRC-005-1 R1 because its previous generation Protection System program documents failed to include a summary of maintenance and testing procedures, and two of its seven previous program documents failed to include maintenance and testing intervals and their basis for voltage and current sensing devices. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because although the entity failed to include summaries of its Protection System maintenance and testing procedures and identify all Protection System devices, the entity still maintained and tested 97.8% of its Protection System devices as required by its Protection System maintenance and testing programs. Therefore, MRO determined that this issue did not pose a serious or substantial risk to the BPS. | The entity reviewed and revised its Protection System maintenance and testing program for generation and transmission Protection Systems in order to consolidate multiple maintenance and testing programs into one program that addresses all of the component types required by PRC-005-1. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 12 (MRO_URE12) | NCRXXXXX | MRO201100311 | PRC-005-1 | R2.1, R2.1 | The entity self-reported noncompliance with Reliability Standard PRC-005-1 R2 because it discovered that it failed to maintain evidence of testing records for 8 current transformers (CTs) and 1 potential transformer (PT). The entity's relay personnel in one location discovered the missing records when they were working with the relay personnel in another location to consolidate the PRC-005 and PRC-008 relays and associated devices into a common database. | MRO determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the devices are associated with transformers that step the voltage down from the BPS to the sub-transmission level. The entity included the devices as BPS devices because some of the CTs tie to the 115 kV differential schemes at the substations. The others are all on the transformer protection that if failed, would result in either a breaker failure scheme, or back-up over current/zone 3 elements on the 115 kV devices. Additionally, all of the relays were tested and documented and performed satisfactorily. | The entity performed the following actions to mitigate the issue: (1) tested the Protection System components identified in the scope of the issue; (2) performed a comprehensive review of the Protection System maintenance and testing records; and (3) upon completing the comprehensive review, performed testing of devices missing evidence of maintenance and testing. |
| Midwest Reliability Organization (MRO) | Unidentified Registered Entity 13 (MRO_URE13) | NCRXXXXX | MRO201000216 | CIP-004-1 | R4.1 | During a CIP Spot Check, conducted jointly by MRO and another Regional Entity, it was determined that the entity was not able to demonstrate that it maintained and reviewed a list of personnel with authorized cyber access to Critical Cyber Assets. The entity did demonstrate that its unescorted physical access list for personnel including contractors and vendors was sufficient. | MRO determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS) because although the entity did not review its list of authorized individuals on a quarterly basis, the individuals were properly authorized and had received cyber security training and personnel risk assessments were conducted prior to granting such access. | This partial period issue was corrected prior to the CIP Spot Check. Subsequently, the entity added granularity to its access tracking spreadsheet which further describes the five types of cyber access it grants. The entity's list is reviewed quarterly and updated within 7 calendar days of any change of personnel with access to Critical Cyber Assets or any change in the access rights of such personnel. |
| Northeast Power Coordinating Council, Inc. (NPCC) | Unidentified Registered Entity 1 (NPCC_URE1) | NCRXXXXX | NPCC201100246 | TOP-002-2a | R14 | The entity self-reported noncompliance with TOP-002-2a R14. NPCC determined that the entity failed to notify the Balancing Authority/Transmission Operator (BA/TOP) of reduction in capabilities due to the poor condition of the fuel. | NPCC determined that there was a minimal risk to the reliability of the bulk power system because although there was an actual reduction in output due to poor condition of fuel, it was minimal, 20 MW (out of approximately 28,000 MW for the entire BA). In addition, the output of this type of plant is commonly variable depending on availability of fuel. Also, the duration for loss of capability was minimal, 11 hours in total for three occurrences on the same day. | The entity's mitigation activities were to: (1) Post a bulleted list of reportable events for an everyday reminder to all operators.<br>(2) Conduct training with the shift supervisors and control room operators. |
| Northeast Power Coordinating Council, Inc. (NPCC) | Unidentified Registered Entity 2 (NPCC_URE2) | NCRXXXXX | NPCC2011007273 | CIP-007-1 | R4 | The entity self-reported noncompliance with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. There were 15 late TFE requests that were filed. The TFE- Part A approval for all was granted by NPCC and NPCC determined that these issues resulted from failures to comply with administrative processes related to the submission of formal TFE requests. | NPCC determined that there was a minimal risk to the reliability of the bulk power system. The entity's system is structured with intrusion prevention sensors at the network and host level, hardened operating systems, strong account management, logging for system configuration changes, and periodic vulnerability scans are run on the devices in question. The compensating measures were in place prior to the due date on which all such TFE requests were to originally have been submitted to NPCC. | The TFE- Part A approval was granted by NPCC. The approved TFE requests are open-ended because the hardened operating system in question does not support third party software. |
| Reliability*First* Corporation (Reliability*First*) | Unidentified Registered Entity 1 (RFC_URE1) Crawfordsville Electric Light and Power (CELP) | NCRXXXXX | RFC201100863 | CIP-003-3 | R2 | The entity submitted a Self-Report to Reliability*First* identifying a possible issue concerning CIP-003-3 R2 because the entity has one senior manager who was approving the implementation of and adherence to the CIP Standards, but failed to identify this individual by name, title, and date of designation as the CIP senior manager. | Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the entity has one senior manager, who was performing the function of a CIP senior manager throughout the duration of the issue by approving the implementation of and adherence to the CIP Standards. In addition, the entity has no Critical Cyber Assets. | The entity designated its senior manager as the CIP senior manager. |
| Reliability*First* Corporation (Reliability*First*) | Unidentified Registered Entity 2 (RFC_URE2) | NCRXXXXX | RFC201000746 | VAR-002-1.1a | R2 | During a compliance audit, Reliability*First* discovered that, based on voltage schedule graphs presented by the entity, the entity operated outside the voltage schedule set by its Transmission Operator. Specifically, the entity failed to operate within the voltage schedule set by its Transmission Operator of 356 kV - 360 kV (358 kV +/- 2 kV). The deviations ranged up to -5 kV outside this schedule. During these time periods, the entity did not have an exemption from its Transmission Operator. | Reliability*First* determined that risk to the reliability of the bulk power system was minimal because the voltage regulators at the entity remained in automatic VAR mode, and therefore could continue to contribute VARs to the bulk power system. In addition, the entity's voltage schedule reflected a relatively narrow bandwidth that did not accurately represent the real-time voltage range in its region. After the issue was identified, the entity worked with its Transmission Operator to modify its voltage schedule to provide a greater bandwidth. As a result, the Transmission Operator expanded the original 356 kV - 360 kV voltage schedule to 345 kV - 360 kV. None of the deviations from the voltage schedule that occurred during the pendency of the issue would have occurred under the new voltage schedule. | The entity requested a modified voltage schedule from its Transmission Operator that more accurately reflects the normal voltage conditions in the area, re-trained control room operators, implemented new distributed control system alarming, and updated its reliability compliance manual for VAR-002 topics. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Reliability*First* Corporation (Reliability*First* ) | Unidentified Registered Entity 3 (RFC_URE3) | NCRXXXXX | RFC201000397 | CIP-004-1 | R4 | During a Spot Check, Reliability*First* determined that the entity failed to include the specific electronic access rights of personnel with authorized cyber access to Critical Cyber Assets on its lists of authorized personnel. The entity maintained two lists of personnel with authorized cyber access to Critical Cyber Assets: a general list of personnel and a list of support personnel. Both of these lists failed to include the specific electronic access rights of personnel with access to Critical Cyber Assets. Reliability*First* determined noncompliance with CIP-004-1 R4 by failing to include the specific electronic access rights of personnel with authorized cyber access to Critical Cyber Assets on its lists of authorized personnel. | Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS). This issue did not result from unauthorized access to Critical Cyber Assets; in fact the personnel on each access list had satisfied all of the requirements for access to Critical Cyber Assets, including the completion of annual cyber security training and personnel risk assessments, in accordance with CIP-004-1. Instead, this issue resulted from the entity's failure to specify the electronic access rights to Critical Cyber Assets within its lists of authorized personnel. Therefore, this was a documentation issue, rather than an instance of unauthorized access. | The entity memorialized the actions it took to address the issue related to CIP-004-1 R4. The entity updated its lists of authorized personnel to include the specific electronic access rights of personnel with authorized access to its Critical Cyber Assets. |
| Reliability*First* Corporation (Reliability*First* ) | Unidentified Registered Entity 3 (RFC_URE3) | NCRXXXXX | RFC201000401 | FAC-009-1 | R1 | During an Audit, Reliability*First* determined that the entity failed to demonstrate that it developed Facility Ratings for generator relay protective devices that were consistent with its Facility Ratings Methodology. Specifically, the entity did not provide evidence of Facility Ratings for generator current transformers. Reliability*First* found that the entity violated FAC-009-1 R1 by failing to establish Facility Ratings consistent with its Facility Ratings Methodology. | Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because the entity confirmed that it had correctly identified the most limiting element in its Facility Ratings prior to its establishment of the generator current transformer Ratings. | The entity calculated the generator current transformer ratings according to its Facility Ratings Methodology, and revised its Facility Ratings documentation to include the generator current transformer Ratings. |
| Reliability*First* Corporation (Reliability*First* ) | Unidentified Registered Entity 3 (RFC_URE3) | NCRXXXXX | RFC201000402 | TPL-001-0.1 | R1 | During an Audit, Reliability*First* discovered an issue with TPL-001-0.1 R1 by concluding that the entity failed to demonstrate that system performance meets Table I for Category A normal conditions (no contingencies). Specifically, the entity failed to provide sufficient evidence to demonstrate that it performed a stability assessment for system performance in accordance with Table I for Category A. While the entity provided a document containing a graph with plot points related to Category B (loss of a single element) and Category C (loss of two or more elements) contingencies, Category A was not included. Furthermore, the entity did not accompany the aforementioned graphical information with an explanation or assessment to demonstrate that the entity evaluated events of Table I for Category A. | Reliability*First* determined that the issue posed a minimal risk to the reliability of the BPS. Although the entity did not produce sufficient documentation at the Audit to establish compliance with TPL-001-0.1 R1, the entity represented that it performed a stability assessment and developed an operating procedure to address items identified in the stability assessment. The entity further represented that it coordinated this operating procedure with its Reliability Coordinator and reviewed the operating procedure on multiple occasions. As part of its mitigation, the entity formally documented the results from its previously completed stability assessment, which demonstrates that this issue was a documentation issue. | The entity documented its previously completed stability assessment results, which demonstrate that system performance meets Table 1 for Category A, and submitted these results to Reliability*First* . |
| Reliability*First* Corporation (Reliability*First* ) | Unidentified Registered Entity 3 (RFC_URE3) | NCRXXXXX | RFC201000403 | TPL-002-0 | R1 | During an Audit, Reliability*First* discovered an issue with TPL-002-0 R1 by concluding that the entity failed to demonstrate that system performance meets Table I for Category B single element contingencies. Specifically, the entity failed to provide sufficient evidence to demonstrate that it performed a stability assessment for system performance in accordance with Table I for Category B contingencies. While the entity provided a graph with plot points related to Category B contingencies, the entity did not accompany the aforementioned graphical information with an explanation or assessment to demonstrate that the entity evaluated events of Table I for Category B contingencies. | Reliability*First* determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the entity did not produce sufficient documentation at the Audit to establish compliance with TPL-002-0 R1, the entity represented that it performed a stability assessment and developed an operating procedure to address items identified in the stability assessment. The entity further represented that it coordinated this operating procedure with its Reliability Coordinator and reviewed the operating procedure on multiple occasions. As part of its mitigation, the entity formally documented the results from its previously completed stability assessment, which demonstrates that this issue was a documentation issue. | The entity documented its previously completed stability assessment results, which demonstrate that system performance meets Category B contingencies, and submitted these results to Reliability*First.* |
| Reliability*First* Corporation (Reliability*First* ) | Unidentified Registered Entity 3 (RFC_URE3) | NCRXXXXX | RFC201000404 | TPL-003-0 | R1 | During an Audit, Reliability*First* discovered an issue with TPL-003-0 R1 by concluding that the entity failed to demonstrate that system performance meets Table I for Category C multiple element contingencies. Specifically, the entity failed to provide sufficient evidence to demonstrate that it performed a stability assessment for system performance in accordance with Table I for Category C contingencies. While the entity provided a graph with plot points related to Category C contingencies, the entity did not accompany the aforementioned graphical information with an explanation or assessment to demonstrate that the entity evaluated events of Table I for Category C contingencies. | Reliability*First* determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Although the entity did not produce sufficient documentation at the Audit to establish compliance with TPL-003-0 R1, the entity represented that it performed a stability assessment and developed an operating procedure to address items identified in the stability assessment. The entity further represented that it coordinated this operating procedure with its Reliability Coordinator and reviewed the operating procedure on multiple occasions. As part of its mitigation, the entity formally documented the results from its previously completed stability assessment, which demonstrates that this issue was a documentation issue. | The entity documented its previously completed stability assessment results, which demonstrate that system performance meets Category C contingencies, and submitted these results to Reliability*First* . |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Reliability*First* Corporation (Reliability*First*) | Unidentified Registered Entity 4 (RFC_URE4) | NCRXXXXX | RFC201000671 | PRC-005-1 | R2.1 | The entity submitted a Self-Report to Reliability*First* concerning an issue related to PRC-005-1 R2 because the entity did not perform maintenance and testing on seven Protection System battery banks within the defined intervals of its Protection Systems maintenance and testing program (Program). While conducting an internal compliance assessment, the entity discovered that it did not perform required maintenance and testing in one quarterly interval for seven battery banks. The maintenance and testing was performed between 10 and 17 days after the defined quarterly interval. The seven battery banks account for approximately 1.2% of the entity's 557 total Protection System devices. The entity confirmed that it did not miss any monthly or five-year battery testing intervals. | Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because: (1) the issue was short in duration (17 days); (2) the entity's Program is more stringent than IEEE's Standard 450 recommended maintenance and testing in that the entity performs maintenance and testing activities four times over the same time period that IEEE Standard 450 recommends for those maintenance and testing activities to occur only once; (3) the entity confirmed that the battery banks were in good condition both prior to and following the missed quarterly battery testing interval; (4) the entity timely completed all monthly battery testing in accordance with its Program, and the entity confirmed from the results of the monthly battery testing that the battery banks were in good condition; and (5) the entity's battery banks have alarms that alert for abnormal conditions, and no abnormal conditions triggered these alarms during the time period of the remediated issue. | The entity completed the quarterly battery testing of its seven battery banks. In addition, the entity conducted PRC-005 training for its facility personnel during which it stressed the importance of testing Protection System devices within the defined intervals, and the potential impact on the BPS of the failure to do so. The entity created a new category within its maintenance management system tracking software by programming logic into the system to capture the defined quarterly battery testing intervals in order to enhance the capabilities of its computerized maintenance management system. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 1 (SERC_URE1) | NCRXXXXX | SERC201000728 | FAC-008-1 | R2 | SERC_URE1 submitted a Self-Report to SERC reporting that it had failed to make its Facility Ratings Methodology (FRM) available for inspection and technical review by the Transmission Planner (TP) within 15 business days of receipt of a request as required. Specifically, SERC_URE1 was asked for its facility rating and how the rating was determined by its TP. SERC_URE1 responded approximately six days after the 15 business day requirement. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because SERC_URE1 had a FRM and a facility rating based on the FRM. The requested methodology was provided by SERC_URE1 to its Transmission Planner 6 days beyond the 15 day requirement in the Standard. | SERC_URE1 completed the following action:<br>(1) Issued an order to personnel and provided training regarding the importance of timely responses for information requests within the 15 business day requirement. The order is kept in a binder and is reviewed when a request is made. Current employees will receive training on an annual basis and the subject matter is included in new hire training.<br>(2) All requests will be logged into SERC_URE1's Compliance calendar, which contains a reminder notification sent prior to the due date. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 2 (SERC_URE2) | NCRXXXXX | SERC2011007527 | CIP-002-2 | R4 | This issue was discovered during a SERC off-site audit. SERC_URE2 was unable to provide a signed and dated record of the senior manager's or delegate's annual approval of the risk-based assessment methodology (RBAM) as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE2 has no Critical Assets (CA) and does not own or operate any facilities that would meet any of the Critical Asset Criteria (CCA) set forth in the proposed CIP-002-4.<br>(2) SERC_URE2 has a documented RBAM. | SERC_URE2 completed the following action: Modified its RBAM procedure to reflect an annual review and approval by the designated and documented senior manager. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 2 (SERC_URE2) | NCRXXXXX | SERC2011007529 | CIP-002-1 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE2 failed to consider all of its assets in the performance of the risk-based assessment methodology (RBAM) as required. Specifically, the evidence showed that 21 of 28 assets were not evaluated using the documented criteria. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE2 has no Critical Assets (CA) and does not own or operate any facilities that would meet any of the Critical Asset Criteria (CCA) set forth in the proposed CIP-002-4.<br>(2) SERC_URE2 has a documented RBAM. | SERC_URE2 completed the following action: Modified its procedure to clearly reflect the use of the RBAM to evaluate and identify CAs and CCAs. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 2 (SERC_URE2) | NCRXXXXX | SERC2011007528 | CIP-003-1 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE2 failed to provide evidence that a single senior manager had been assigned with overall responsibility and authority for CIP-002 through CIP-009 as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4. | SERC_URE2 completed the following action: Assigned a senior manager with the overall responsibility and authority for leading and managing the implementation of and adherence to the CIP-002 through CIP-009. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 3 (SERC_URE3) Blue Ridge Electric Membership Corporation (Blue Ridge) | NCRXXXXX | SERC2011007290 | CIP-003-1 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE3 failed to provide evidence that a designated senior manager was assigned responsibility for CIP-002 through CIP-009 as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) SERC_URE3 has no critical assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4.<br>(2) SERC_URE3 is a minimal size utility. | SERC_URE3 completed the following action: Revised its documentation to reflect that a single senior manager, identified by name, title, date of designation and contact information, is responsible for implementation and adherence to CIP-002 through CIP-009. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 3 (SERC_URE3) Blue Ridge Electric Membership Corporation (Blue Ridge) | NCRXXXXX | SERC2011007282 | CIP-002-2 | R4 | This issue was discovered during a SERC off-site audit. SERC_URE3 was unable to provide a signed and dated record of the senior manager's or delegate's annual approval of the risk-based assessment methodology (RBAM) as required by the Standard for 2010. Specifically, SERC_URE3 established that its RBAM was reviewed and approved as required for 2009 and 2011. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE3 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4.<br>(2) SERC_URE3 has a documented RBAM. | SERC_URE3 completed the following action: Revised its Memorandum to reflect that on an annual basis, the RBAM will be reviewed, approved by the designated and documented Senior manager for compliance, and will be used to identify critical and cyber assets. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 4 (SERC_URE4) | NCRXXXXX | SERC201000495 | PRC-008-0 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE4 failed to provide evidence that its UFLS Maintenance and Testing Program was properly implemented as required by PRC-008-0 R2. SERC_URE4 was unable to provide evidence that the under frequency element of the electronic re-closer control relays had been tested. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE4's Transmission Owner/Transmission Operator has its own protective relaying. In addition, SERC_URE4 owns protective relaying to protect SERC_URE4-owned equipment on the SERC_URE4 side of the delivery point. Because of this configuration, it is unlikely that an event occurring on the SERC_URE4 electric system would affect the BPS.<br>(2) SERC_URE4 is a minimal size utility. Because SERC_URE4 is connected radially, it would have little impact on the BPS if an underfrequency event had occurred. | SERC_URE4 completed the following actions:<br>(1) Established a program that identified the UFLS equipment and defined the maintenance and testing schedule.<br>(2) Tested its UFLS equipment. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 4 (SERC_URE4) | NCRXXXXX | SERC2011006700 | PRC-008-0 | R1 | SERC_URE4 submitted a Self-Report to SERC reporting that it had failed to have a UFLS equipment maintenance and testing program as required by PRC-008-0 R1. SERC_URE4 did not have a written procedure addressing UFLS equipment identification as well as a schedule for UFLS equipment testing and maintenance. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE4's Transmission Owner/Transmission Operator has its own protective relaying. In addition, SERC_URE4 owns protective relaying to protect SERC_URE4-owned equipment on the SERC_URE4 side of the delivery point. Because of this configuration, it is unlikely that an event occurring on the SERC_URE4 Electric System would affect the BPS.<br>(2) SERC_URE4 is a minimal size utility. Because SERC_URE4 is connected radially, it would have little impact on the BPS if an underfrequency event had occurred. | SERC_URE4 completed the following actions:<br>(1) Established a program that identified the UFLS equipment and defined the maintenance and testing schedule.<br>(2) Tested its UFLS equipment. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 5 (SERC_URE5) Haywood Electric Membership Corporation (Haywood) | NCRXXXXX | SERC2011007283 | CIP-003-1 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE5 failed to provide evidence that a single senior manager had been assigned with overall responsibility and authority for CIP-002 through CIP-009 as required. SERC_URE5 created a procedure designating the responsibility and authority to a senior manager, who was identified by name, title, business phone and business address. This is a gap issue. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) SERC_URE5 has no Critical Assets.<br>(2) H69SERC_URE5 does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4. | SERC_URE5 completed the following action: assigned a single senior manager with overall responsibility for compliance with CIP-002 through CIP-009. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 6 (SERC_URE6) | NCRXXXXX | SERC2011006593 | CIP-004-1 | R4 | SERC_URE6 submitted a Self-Report to SERC reporting that it had 12 out of 191 individuals who were omitted or incorrectly documented in its Critical Cyber Asset access lists. Also, one contracted custodian was authorized for one Physical Security Perimeter (PSP) list, but was inadvertently given access to two PSP lists and used this access for a total of 41 days. One of the employees accessed the PSP but had a current PRA and cyber security training. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) All of the omitted individuals possessed current training Personal Risk Assessments.<br>(2) All of the omitted individuals possessed current CIP training credentials.<br>(3) All individuals had a valid business need for their access. | SERC_URE6 completed the following actions:<br>(1) Remedied all of the identified discrepancies in the existing CCA access lists<br>(2) Created a new electronic access request form and request for change approval tool regarding access privileges to CCAs.<br>(3) Sent an awareness communication to personnel involved in granting and approving access to CCAs and maintaining CCA access lists.<br>(4) Implemented a quality assurance review process for all grants of unescorted physical access to CCAs. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 7 (SERC_URE7) Lockhart Power Company (Lockhart) | NCRXXXXX | SERC2011007393 | CIP-001-1a | R3 | SERC_URE7 submitted a Self-Report to SERC reporting that it did not provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events by the beginning of the enforceable period for SERC_URE7. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE7 is a minimal size utility. SERC_URE7 is connected radially to the BPS at three interconnection points. SERC_URE7 does not own or operate any BPS facilities.<br>(2) The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS would be recognized and reported by the TO/TOP. | SERC_URE7 completed the following action: Provided operating personnel with it sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 8 (SERC_URE8) | NCRXXXXX | SERC2011007445 | FAC-008-1 | R1 | This issue was discovered during a SERC on-site audit. SERC_URE did not address series and shunt compensation devices in its Facility Rating Methodology (FRM) as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) SERC_URE8's FRM was designed to reflect the most limiting element, the Current Transformer.<br>(2) While SERC_URE8 failed to include series and shunt compensation devices in its FRM, it has never owned series and shunt compensation devices. | SERC_URE8 completed the following action: Revised its FRM to include consideration statements for all the devices listed in the Standard. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 9 (SERC_URE9) | NCRXXXXX | SERC2011007536 | CIP-001-1 | R1 | This issue was discovered during a SERC on-site audit. SERC_URE9 failed to have procedures for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE9 does not own or operate any BPS equipment.<br>(2) SERC_URE9 is a minimal size utility.<br>(3) SERC_URE9 did have a security policy in place prior to June 18, 2007; however, it did not address the specific requirements of R1. | SERC_URE9 completed the following action: Modified its security policy to:<br>(1) Include provisions for making operating personnel aware of sabotage events.<br>(2) Provide the process for communicating information on sabotage events to appropriate parties in the Interconnection.<br>(3) Provide personnel with the sabotage response guidelines. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 9 (SERC_URE9) | NCRXXXXX | SERC2011007537 | CIP-001-1 | R2 | This issue was discovered during a SERC on-site audit. SERC_URE9 failed to have a procedure for the communication of information concerning sabotage events to appropriate parties in the Interconnection. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE9 does not own or operate any BPS equipment.<br>(2) SERC_URE9 is a minimal size utility.<br>(3) SERC_URE9 did have a security policy in place prior to June 18, 2007; however, it did not address the specific requirements of R1. | SERC_URE9 completed the following action: Modified its security policy to:<br>(1) Include provisions for making operating personnel aware of sabotage events.<br>(2) Provide the process for communicating information on sabotage events to appropriate parties in the Interconnection.<br>(3) Provide personnel with the sabotage response guidelines. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 9 (SERC_URE9) | NCRXXXXX | SERC2011007538 | CIP-001-1 | R3 | This issue was discovered during a SERC on-site audit. SERC_URE9 failed to provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE9 does not own or operate any BPS equipment.<br>(2) SERC_URE9 is a minimal size utility.<br>(3) SERC_URE9 did have a security policy in place prior to June 18, 2007; however, it did not address the specific requirements of R1. | SERC_URE9 completed the following action: Modified its security policy to:<br>(1) Include provisions for making operating personnel aware of sabotage events.<br>(2) Provide the process for communicating information on sabotage events to appropriate parties in the Interconnection.<br>(3) Provide personnel with the sabotage response guidelines. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 9 (SERC_URE9) | NCRXXXXX | SERC2011006763 | CIP-002-1 | R4 | This issue was discovered during a SERC off-site audit. SERC_URE9 failed to sign and date its annual approval of the list of Critical Assets (CA) and the list of Critical Cyber Assets (CCA) as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE9 has no Critical Assets.<br>(2) SERC_URE9 does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4.<br>(3) SERC_URE9 does not own or operate any BPS equipment. | SERC_URE9 completed the following action: Created a procedure requiring the designated senior manager to review and approve the risk-based assessment methodology, CA and CCA lists on an annual basis and establishing a retention policy for the signed and dated CA and CCA approval lists. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 9 (SERC_URE9) | NCRXXXXX | SERC2011006764 | CIP-003-1 | R2 | This issue was discovered during a SERC off-site audit. SERC_URE9 failed to provide evidence that a single senior manager had been assigned overall responsibility and authority for CIP-002 through CIP-009 as required. SERC_URE9 put a procedure in place in June 2010; however; it did not contain the title, business phone and business address of the senior manager as required. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because:<br>(1) SERC_URE9 has no Critical Assets.<br>(2) SERC_URE9 does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4.<br>(3) SERC_URE9 does not own or operate any BPS equipment. | SERC_URE9 completed the following action: Developed a written document assigning responsibility for CIP-002 through CIP-009 to a senior manager identified. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 10 (SERC_URE10) | NCRXXXXX | SERC201100745 | CIP-005-1 | R1 | SERC_URE10 submitted a Self-Report to SERC reporting that it had failed to appropriately classify an asset as a non critical Cyber Asset within a defined Electronic Security Perimeter (ESP). Specifically, when applying the methodology, personnel did not realize the asset was located on a network with Critical Cyber Assets (CCA) that utilize a routable protocol. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) The device was a hardened appliance that was utilized to monitor the network performance and system logging.<br>(2) The appliance resided within the Physical Security Perimeter, which requires CIP 4 credentials or escorted access in order to gain physical access. | SERC_URE10 completed the following actions:<br>(1) Removed the asset from the ESP.<br>(2) Updated its CCA Identification Training to further clarify how to identify non-critical cyber assets within the ESP.<br>(3) Trained its staff on the new CCA Identification process.<br>(4) Created and reviewed with impacted business units the instructional procedure for the required annual CCA review. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 11 (SERC_URE11) | NCRXXXXX | SERC200900342 | CIP-004-1 | R2 | SERC_URE11 submitted a Self-Report to SERC reporting that it had retained an employee on the list that would have allowed access to a Control Center when the employee did not possess the required Cyber Security training. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the employee had been working for the entity for more than six years at the time of the incident. | SERC_URE11 completed the following actions:<br>(1) Revoked card access allowing physical entry to the Control Center for the five identified employees was revoked.<br>(2) Completed a personnel risk assessment and associated training for one of the five employees was completed to enable job required access to the Control Center.<br>(3) Created a written procedure establishing a quarterly review of personnel having physical access to Critical Cyber Assets, including the Control Center that takes place within 5 calendar days of the end of a calendar year quarter. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 11 (SERC_URE11) | NCRXXXXX | SERC200900343 | CIP-004-1 | R3 | SERC_URE11 submitted a Self-Report to SERC reporting that it had allowed an employee, who did not possess the required Personnel Risk Assessment, to retain physical access to a Control Center. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the employee had been working for the entity for more than six years month at the time of the incident. | SERC_URE11 completed the following actions:<br>(1) Revoked card access allowing physical entry to the Control Center for the five identified employees was revoked.<br>(2) Completed a personnel risk assessment and associated training for one of the five employees was completed to enable job required access to the Control Center.<br>(3) Created a written procedure establishing a quarterly review of personnel having physical access to Critical Cyber Assets, including the Control Center that takes place within 5 calendar days of the end of a calendar year quarter. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 11 (SERC_URE11) | NCRXXXXX | SERC200900344 | CIP-004-1 | R4 | SERC_URE11 submitted a Self-Report to SERC reporting that it had allowed four employees who were not included on the authorized cyber or authorized unescorted physical access lists to have access to Critical Cyber Assets. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the persons involved at the time of the of the incident were long term employees. | SERC_URE11 completed the following actions:<br>(1) Revoked card access allowing physical entry to a Control Center for the five identified employees was revoked.<br>(2) Completed a personnel risk assessment and associated training for one of the five employees was completed to enable job required access to a Control Center.<br>(3) Created a written procedure establishing a quarterly review of personnel having physical access to Critical Cyber Assets, including a Control Center, that takes place within 5 calendar days of the end of a calendar year quarter. |
| SERC Reliability Corporation (SERC) | Unidentified Registered Entity 12 (SERC_URE12)Tilton Energy, LLC (Tilton Energy) | NCRXXXXX | SERC2011007153 | CIP-003-3 | R2 | This issue was discovered during a SERC on-site audit. SERC_URE12 was not able to establish the date of the delegate's designation as required by the Standard. | SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because:<br>(1) SERC_URE12 has no Critical Assets.<br>(2) SERC_URE12 does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4. | SERC_URE12 completed the following action: Modified its procedure to include the date of designation of the delegate. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 1 (SPP_URE1) | NCRXXXXX | SPP200900104 | FAC-008-1 | R1 | In a Compliance Audit, it was found that the relays protective devices and instrument transformers were not considered in SPP_URE1's Facility Ratings Methodology. Additionally, SPP_URE1's protective relays were not considered in its Facility Ratings Methodology. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE1 did not consider its relays protective devices and instrument transformers in its facility rating methodology, the relay protective devices and instrument transformers were not a limiting element in the design of SPP_URE1's generation facility and did not impact the capacity rating of its generation facility. | SPP_URE1 revised its Facility Ratings Methodology to include the ratings for instrument transformers and protective relays, assigning them a rating based on original equipment manufacturer ratings. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 1 (SPP_URE1) | NCRXXXXX | SPP200900105 | FAC-009-1 | R1 | In a Compliance Audit, it was found that SPP_URE1 listed the nameplate ratings of the components of its facility in its Facility Ratings Methodology, but did not identify the most limiting element. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). SPP_URE1's rating of its generation facility is based on the design rating of the facility. SPP_URE1's failure to document the most limiting element did not impact the rating of its facility. | SPP_URE1 revised its plant procedure to include individual equipment ratings for instrument transformers and protective relays, and to include a separate statement identifying the most limiting equipment rating for its Facility and the Facility Rating. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 2 (SPP_URE2) | NCRXXXXX | SPP201000213 | CIP-007-1 | R5.3 | In a self-report, SPP_URE2 indicated that a password on its legacy SCADA system (a Critical Cyber Asset) was non-compliant with CIP-007-1 R5.3 because (1) it did not incorporate six characters per R5.3.1; (2) did not include a combination of alpha, numeric, and "special characters" per R5.3.2; and (3) was not changed annually per R5.3.3. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although the root administrator password on SPP_URE2's legacy SCADA system (a Critical Cyber Asset) was non-compliant, the user access passwords that were used to access the legacy SCADA application addressed the requirements of CIP-007-1 R5.3. Further, SPP_URE2 utilized an outside security service that would detect and alarm any attempts at unauthorized access to the SCADA system. This combination of user access password requirements and unauthorized access monitoring established a redundant shield against unauthorized intrusions. | SPP_URE2 submitted a TFE, which was subsequently accepted and approved. An upgrade of the legacy SCADA system was installed and the new system addresses the requirements of CIP-007-1 R5.3. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 3 (SPP_URE3) | NCRXXXXX | SPP201000254 | PRC-005-1 | R1 | In a Compliance Audit, it was found that SPP_URE3's relay maintenance and testing procedure lacked the following: testing intervals and the basis for intervals for CTs and PTs; testing intervals and the basis for intervals for associated communications systems; and the basis for battery testing intervals. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS) because SPP_URE3 was testing and monitoring the protection system devices that were missing from its Protection System Testing and Maintenance Program through its SCADA system. SPP_URE3 was also testing its batteries according to the intervals in its plan, testing its voltage and current sensing devices simultaneously with its relays, most of which are monitored through its SCADA system, and routinely inspecting its substations, which includes checks of these devices. Finally, SPP_URE3 was monitoring its associated communication systems through its SCADA system; testing, end to end, its channel signal strength daily, beginning at 4 a.m. and continuing until all channels are tested successfully; testing, through a low and high power test, how communications would function at half power; and performing a functional end to end testing with another entity, either at its request or at least annually. | SPP_URE3's protection system maintenance and testing procedures were revised to include testing intervals for all required elements, as well as the basis for those intervals. Standardized inspection and testing forms were developed. Applicable staff of SPP_URE were trained on the revised procedures. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 3 (SPP_URE3) | NCRXXXXX | SPP201000405 | PRC-004-1 | R1 | In a Self Certification, SPP_URE3 reported that its procedures for analyzing and mitigating transmission Protection Systems Misoperations were deficient. The procedures did not include sufficient detail and did not identify the responsible personnel assigned to perform each step in the process. The procedures also did not clearly define what constitutes a misoperation, leading to discrepancies in understanding between employees. As a result, not all potential misoperations were being logged, monitored, and evaluated. | SPP RE determined that the issue posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). SPP_URE3 was not evaluating all of its potential misoperations; therefore, the SPP_URE3 system was vulnerable to the extent that SPP_URE3 could have recurring misoperations or the applicable devices would not operate appropriately when required to do so. This poses a moderate risk to the BPS because misoperations were not correctly identified and corrected. | The Registered Entity developed a new procedure that clearly identifies the steps to be taken to identify Misoperations and to implement corrective action plans. A tracking tool was developed for documenting potential misoperations, the investigation that was performed, and any corrective action that was taken. A training program was implemented to train employees on the new procedure and the use of the tracking tools. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 3 (SPP_URE3) | NCRXXXXX | SPP201000406 | PRC-004-1 | R2 | In a Self Certification, SPP_URE3 reported that its procedures for analyzing and mitigating generation Protection Systems Misoperations were deficient. The procedures did not include sufficient detail and did not identify the responsible personnel assigned to perform each step in the process. The procedures also did not clearly define what constitutes a misoperation, leading to discrepancies in understanding between employees. As a result, not all potential misoperations were being logged, monitored, and evaluated. | SPP RE determined that the issue posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS).SPP_URE3 was not evaluating all of its potential misoperations; therefore, the SPP_URE3 system was vulnerable to the extent that SPP_URE3 could have recurring misoperations or the applicable devices would not operate appropriately when required to do so. This poses a moderate risk to the BPS because misoperations were not correctly identified and corrected. | The Registered Entity developed a new procedure that clearly identifies the steps to be taken to identify Misoperations and to implement corrective action plans. A tracking tool was developed for documenting potential misoperations, the investigation that was performed, and any corrective action that was taken. A training program was implemented to train employees on the new procedure and the use of the tracking tools. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 4 (SPP_URE4) | NCRXXXXX | SPP201000300 | CIP-002-1 | R3 | In a Spot Check, it was found that SPP_URE4's Critical Cyber Asset (CCA) list included four switches that were located logically outside the Electronic Security Perimeter. The switches were not essential to the function of the Critical Asset and should not have been included on the CCA list. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The four Cisco switches that had been included on the list of CCAs for SPP_URE4 did not, in fact, qualify as CCAs and, therefore, should not have been included on the list of CCAs. Because the four switches were the only "CCAs" located outside the ESP, and because the switches are not, in fact, CCAs, no CCAs were left unprotected or were subject to compromise. | SPP_URE4 updated its CCA list and the four switches were removed. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 5 (SPP_URE5) | NCRXXXXX | SPP201000350 | CIP-007-1 | R2 | SPP_URE5 self reported that as a result of a Vulnerability Assessment, the configuration review of its electronic ports and services showed that one of the systems is not appropriately 'hardened', i.e., not all unnecessary services were disabled, ensuring that authentication to the system, or enumeration protection of information related to the system, were adequate. The configurations for the network devices responsible for CCA communications did not have some of their services disabled, in violation of this Standard.<br>The identified services did not appear to be necessary and should have been disabled to reduce the footprint of the devices on the network. Should a vulnerability be discovered in one of these services, the risk could be mitigated by disabling the service. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). The unnecessary ports and services were open on routers only and not on Critical Cyber Assets within the ESP. Furthermore, event logs sampled did not list these services as activated prior to them being disabled. | SPP_URE5 disabled the ports and services in question on its network devices responsible for CCA communications. By disabling these devices, SPP_URE5 prevented the possibility of any of these devices causing a cyber vulnerability. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 5 (SPP_URE5) | NCRXXXXX | SPP201000351 | CIP-007-1 | R3 | SPP_URE5 self reported that it does not currently have a patch management procedure in place for third party applications installed on Critical Cyber Assets. The processes for network patch management and updates were performed informally and were not documented. SPP_URE5 was using an application to identify vulnerabilities in third party applications. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE5 had not documented when it performed its process for network patch management and updates, the patch management and updates were, nonetheless, being performed. The performance of the management and updating is what minimized the risk to the BES. The lack of documentation did not impact the BES enough to raise the risk beyond minimal. | SPP_URE5 incorporated checks for security concerns into a tracking system to generate automated tickets, and these tickets are updated and closed once completed. Patches not applicable are not be installed and are documented within the ticket. The network operating system was updated on applicable devices. Any devices which do not support the latest network operating system were documented and known vulnerabilities have been documented and mitigated. Scans are to be used as a identification and verification component of this procedure. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 6 (SPP_URE6) | NCRXXXXX | SPP201100581 | TOP-002-2a | R3 | SPP_URE6 submitted a self report, reporting the following: Pursuant to the requirements of TOP-002-2a R3, SPP_URE6 regularly provides to its Balancing Authority, Transmission Service Provider, and Transmission Operator a next-day generation availability report and a next-day load forecast. These items are normally transmitted via electronic mail. On a Saturday, SPP_URE6's operations shift supervisor sent email messages to the Balancing Authority and Transmission Operator attaching the generation availability report and load forecast and believed that those items were transmitted successfully. However, when preparing the report and forecast for transmittal the following day (i.e., the Sunday report and forecast reflecting next-day information for Monday), the operations shift supervisor discovered that the Saturday messages had not been successfully transmitted. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Upon discovering that the generation availability report and load forecast for Saturday (containing next-day information for Sunday) were not successfully transmitted, SPP_URE6 immediately transmitted both items. SPP_URE6 has a telemetering link with its Balancing Authority and Transmission Operator, which would have permitted this entity to observe information concerning the SPP_URE6 electric system, including its load and generation status, in real-time. Moreover, SPP_URE6's Balancing Authority and Transmission Operator did not contact SPP_URE6 to inquire as to the status of these items, suggesting that its not having received either the day-ahead availability report or day-ahead load forecast did not adversely affect its ability to plan for normal operations on a next-day basis. Finally, the unsuccessful e-mail containing the next-day information did not include current-day or seasonal operations reports. | In order to correct a self-reported issue with NERC Reliability Standard TOP-002-2a, Requirement R3, SPP_URE6 undertook the following measures:<br>(1) Transmitted the Saturday generation availability report and load forecast on Sunday.<br>(2) Implemented revised procedures to ensure that the generation availability report and load forecast are transmitted on a daily basis and that successful transmittal is confirmed.<br>(3) Provided training to operations personnel regarding SPP_URE6's procedures and Reliability Standard TOP-002-2a, Requirement R3. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 6 (SPP_URE6) | NCRXXXXX | SPP201100582 | TOP-003-0 | R1 | SPP_URE6 submitted a self report, reporting the following: Pursuant to the requirements of TOP-003-0 R1, SPP_URE6 provides to its Balancing Authority and Transmission Operator a next-day generation availability report that lists any units that are scheduled to be unavailable for the next day. This report is normally transmitted via electronic mail in accordance with outage reporting requirements established by the Balancing Authority and Transmission Operator. On a Saturday SPP_URE6's operations shift supervisor sent an email message to the Balancing Authority and Transmission Operator attaching the generation availability report for the next day indicating that one unit was scheduled to be unavailable. The operations shift supervisor believed that the report had been transmitted successfully. However, when preparing the report for transmittal the following day (i.e., the Sunday report reflecting next-day information for Monday), the operations shift supervisor discovered that the Saturday report had not been successfully transmitted. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Upon discovering that the generation availability report for Saturday (containing next-day information for Sunday) was not successfully transmitted, SPP_URE6 immediately transmitted the report. SPP_URE6 did not operate any of the units reflected on the availability report on either Saturday or Sunday. Similarly, SPP_URE6 was not directed by its Balancing Authority and Transmission Operator to operate any of the units, including the outaged unit, on these dates. | In order to correct a self-reported issue with NERC Reliability Standard TOP-003-0, Requirement R1, SPP_URE6 undertook the following measures:<br>(1) Transmitted the Saturday generation availability report on Sunday.<br>(2) Implemented revised procedures to ensure that the generation availability report is transmitted on a daily basis and that successful transmittal is confirmed.<br>(3) Provided training to operations personnel regarding SPP_URE6's procedures and Reliability Standard TOP-003-0, Requirement R1. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 6 (SPP_URE6) | NCRXXXXX | SPP201100583 | TOP-006-1 | R1.1 | SPP_URE6 submitted a self report, reporting the following . Pursuant to the requirements of TOP-006-1 R1.1, SPP_URE6 regularly provides to its Balancing Authority and Transmission Operator a next-day generation availability report that lists the generation resources that are available for the next day. This report is normally transmitted via electronic mail in accordance with reporting requirements established by the Balancing Authority and Transmission Operator. On a Saturday, SPP_URE6's operations shift supervisor sent an email message attaching the generation availability report for the next day. The operations shift supervisor believed that the report had been transmitted successfully. However, when preparing the report for transmittal the following day (i.e., the Sunday report reflecting next-day information for Monday), the operations shift supervisor discovered that the Saturday report had not been successfully transmitted. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Upon discovering that the generation availability report for Saturday (containing next-day information for Sunday) was not successfully transmitted, SPP_URE6 immediately transmitted the report. SPP_URE6 did not operate any of the units reflected on the availability report on either Saturday or Sunday. Similarly, SPP_URE6 was not directed to operate any of the units on these dates. | In order to correct a self-reported issue with NERC Reliability Standard TOP-006-1, Requirement R1.1, SPP_URE6 undertook the following measures:<br>(1) Transmitted the Saturday generation availability report on Sunday.<br>(2) Implemented revised procedures to ensure that the generation availability report is transmitted on a daily basis and that successful transmittal is confirmed.<br>(3) Provided training to operations personnel regarding SPP_URE6's procedures and Reliability Standard TOP-006-1, Requirement R1.1. |
| Southwest Power Pool Regional Entity (SPP) | Unidentified Registered Entity 7 (SPP_URE7) | NCRXXXXX | SPP201100585 | TOP-002-2a | R3 | SPP_URE7 submitted a self report, indicating the following statements. Pursuant to the requirements of TOP-002-2a R3, another entity, on its own behalf and on the behalf of SPP_URE7, regularly provides to the utility that serves as the Balancing Authority and Transmission Operator for the other entity and SPP_URE7 systems a next-day load forecast. This item is normally transmitted via electronic mail. On Saturday, the other entity's operations shift supervisor sent an email message to the Balancing Authority and Transmission Operator attaching the load forecast for SPP_URE7 and believed that this item was transmitted successfully. However, when preparing the forecast for transmittal the following day (i.e., the Sunday forecast reflecting next-day information for Monday), the operations shift supervisor discovered that the Saturday message had not been successfully transmitted. | SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Upon discovering that the load forecast for Saturday (containing next-day information for Sunday) was not successfully transmitted, the other entity, on behalf of SPP_URE7, immediately transmitted this item. SPP_URE7 has (via the other entity) a telemetering link with its Balancing Authority and Transmission Operator, which would have permitted the observation of information concerning the SPP_URE7 electric system, including its load, in real-time. Moreover, the Balancing Authority and Transmission Operator did not contact the other entity or SPP_URE7 to inquire as to the status of the load forecast, suggesting that its not having received SPP_URE7's day-ahead load forecast did not adversely affect its ability to plan for normal operations on a next-day basis. Finally, the unsuccessful e-mail containing the next-day information did not include current-day or seasonal operations reports. | Proposed Mitigation Plan:<br>In order to correct a self-reported issue with NERC Reliability Standard TOP-002-2a, Requirement R3, the following measures were undertaken by the other entity and/or SPP_URE7, as applicable:<br>(1) The other entity transmitted the Saturday load forecast on Sunday.<br>(2) The other entity implemented revised procedures to ensure that the load forecast is transmitted on a daily basis and that successful transmittal is confirmed. The procedures included copying SPP_URE7 personnel on such transmittals.<br>(3) SPP_URE7 implemented a procedure to verify that the other entity has transmitted the daily load forecast. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 1 (TRE_URE1) Texas-New Mexico Power Co (TNMP) | NCRXXXXX | TRE201100262 | CIP-003-2 | R1 | TRE_URE1's self-reported that its Cyber Security policy document did not address all requirements of CIP-002When examining TRE_URE1's Cyber Security policy in place at the beginning of the audit period, Texas RE concluded that the following deficiencies existed:<br><br>• Did not address identifying or documenting a risk-based assessment in accordance with CIP-002-3, R1.<br>• Did not directly address the identification of "Critical Asset", in reference to the NERC definition of "Critical Asset". This is deficient in accordance with CIP-002-3, R2.<br>• Did not directly address the identification of "Critical Cyber Asset", in reference to the NERC definition of "Critical Cyber Asset". This is deficient in accordance with CIP-002-3, R3.<br>• Did not address the requirement for annual approval of the risk-based methodology in accordance with CIP-002-3, R4. | This issue did not pose a serious or substantial risk and posed a minimal actual and potential risk to the bulk power system because TRE_URE1 had identified and documented a risk-based assessment methodology (RBAM), performed its RBAM, identified the Critical Asset and Critical Cyber Asset (CCA) lists and all were approved by a senior manager. In addition, the Cyber Security policy was made readily available to all personnel who had access to or who were responsible for CCAs. | This issue had already been mitigated by the time of the audit; the issue represents a deficiency with TRE_URE1's Cyber Security policy at the date of registration.<br><br>New Cyber Security policy was in place at the time of the audit, and it included the items missing in the original document.<br><br>In addition, to the modifications to policy statements within the Cyber Security policy document, a supplement was added to explicitly cross reference each CIP requirement with the corresponding policy statement(s), thus demonstrating that the policy addresses each of the CIP requirements. The addition of this cross reference feature within the document provides documentation that the policy not only addresses all the requirements within CIP-002 through CIP-009 but also provides a mechanism to ensure the policy will continue to align with the CIP standards throughout each review and/or update. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 2 (TRE_URE2) Wharton County Generation, LLC (Wharton County) | NCRXXXXX | TRE201000101 | CIP-001-1 | R2 | As a result of an Audit, Texas RE determined that TRE_URE2 did not have procedures in place for the communication of information concerning all sabotage events with its Qualified Scheduling Entity (QSE). The audit team discovered TRE_URE2's reporting procedure to be insufficient evidence due to lack of detailing when plant operators should notify their QSE in the event of a sabotage. The QSE is the entity then required to communicate any sabotage events to the Reliability Coordinator. The procedure did not state which steps the plant operator(s) should take in the event of a sabotage event. The reporting procedure in place at the time of the audit stated that the plant operator must report sabotage to the Reliability Coordinator, but only for events that are determined to be reportable to State Regulatory Agencies or the Department of Energy. | This issue did not pose a serious or substantial and posed a minimal actual and potential risk to the bulk power system (BPS) because the sabotage reporting procedure contained steps to contact the local area Transmission Owner and who at the time, was performing some of the functions of the Transmission Operator. Texas RE also considered the size and location of the TRE_URE2 facility which produces a moderate amount of generation at approximately 80 MW and because the procedure did require immediate contact with the local area Transmission Operator an incident may have minimal effects of transfer across the BPS interfaces. In addition, the reporting procedure was made available to operating personnel. | TRE_URE2's reporting procedure was updated to include directions for the operators to notify all appropriate parties. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 3 (TRE_URE3) | NCRXXXXX | TRE201000100 | CIP-004-1 | R4 | During a quarterly review, TRE_URE3 discovered that a manually kept aggregated list of personnel with authorized cyber or authorized unescorted physical access to Critical Assets (CA) and Critical Cyber Assets (CCA) was not timely updated when access was granted/revoked for 30 individuals. TRE_URE3 self-reported this issue, stating that nine (9) individuals were given physical access but not added to list within seven days, twelve (12) individuals whose physical access had been revoked were not removed from the list within seven days, and nine (9) individuals were given electronic access but not added to the list within seven days. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because only personnel who had personal risk assessment (PRA) and Cyber Security Training had access at all times. The list subject to the non-compliance does not determine access to CCA's; Access is granted or denied from separate lists that were updated with the correct personnel names and access within the required timeframe. | Computer program written for verifying the access list is current. TRE_URE3 made the following changes in office procedures: (1) data center access request form modified to include a review by a Cyber Security staff member at the control center, (2) Security will now notify the Cyber Security staff member at the control center when any change is made to physical access list, (3) to prevent recurrence, automated alerts are to issued Cyber Security staff member at the control center are generated whenever changes to access are made. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 4 (TRE_URE4) | NCRXXXXX | TRE201000164 | PRC-001-1 | R5 | TRE_URE4 self- reported that when a technician was at a substation installing a disturbance monitoring panel that required drilling holes in the floor, the technician disabled both primary and backup relaying on a 345 kV line in the adjacent panel to mitigate the risk of an operation due to the vibration of the drilling without notifying its Transmission Operator (TOP) in advance of changes to the operating conditions, per TRE_URE4's procedures. Relaying was disabled four minutes prior to notifying the registered TOP. | This issue did not pose a serious or substantial risk and posed a moderate potential and minimal actual risk to the bulk power system for two reasons: (1) The issue period was brief. The Transmission Operator was notified four minutes after the Protection System was disabled. The probability of a fault occurring in four minutes is not high, and (2) Only a portion of the transmission line protection system was disabled. If a fault had occurred on the line, high-speed clearing of the fault would still have occurred.<br>Also, the entity had a procedure in place that if followed by personnel would have prevented the non-compliance. | All field technicians and transmission coordinators were retrained regarding proper notification procedures. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 5 (TRE_URE5) | NCRXXXXX | TRE201100288 | FAC-008-1 | R1 | As a result of an Audit, Texas RE determined that TRE_URE5 did not have a Facility Ratings Methodology (FRM) until the date of its first Facility Ratings Methodology. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the entity was using the regional requirements for determining facility ratings and was providing ratings to the Reliability Coordinator for the facility during the period. | TRE_URE5 had a FRM and the FRM currently in use addresses the requirements of FAC-008 and its use is required by TRE_URE5's own procedures. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 6 (TRE_URE6) City of Boerne | NCRXXXXX | TRE201100303 | CIP-001-1 | R2 | As a result of an Audit, Texas RE determined that the TRE_URE6 failed to have procedures in effect for compliance to CIP-001 R2, R3, and R4 from when it was registered until its procedure was developed in 2010. A CIP-001 procedure was developed before registration date but the entity did not distribute it to their personnel until late 2010. The Entity was using an emergency procedure that included awareness of some sabotage events that specifically covered terrorist attacks. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the entity had a deficient procedure in place that covered potential terrorist attacks. The procedure did include contact information for appropriate parties in the Interconnection. Texas RE also considered the size of the entity and its impact on the system. The entity is responsible for a small amount of generation, approximately 30 MW on its system. | The current procedures address the requirements of CIP-001 and personnel were trained on current procedure. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 6 (TRE_URE6) City of Boerne | NCRXXXXX | TRE201100304 | CIP-001-1 | R3 | As a result of an Audit, Texas RE determined that the TRE_URE6 failed to have procedures in effect for compliance to CIP-001 R2, R3, and R4 from when it was registered until its procedure was developed in 2010. A CIP-001 procedure was developed before registration date but the entity did not distribute it to their personnel until late 2010. The TRE_URE6 was using an emergency procedure that included awareness of some sabotage events with that specifically covered terrorist attacks. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the entity had a deficient procedure in place that covered potential terrorist attacks. Texas RE also considered the size of the entity and its impact on the system. The entity is responsible for a small amount of generation, approximately 30 MW on its system. | The current procedures address the requirements of CIP-001 and personnel were trained on current procedure. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 6 (TRE_URE6) City of Boerne | NCRXXXXX | TRE201100305 | CIP-001-1 | R4 | As a result of an Audit, Texas RE determined that the TRE_URE6 failed to have procedures in effect for compliance to CIP-001 R2, R3, and R4 from when it was registered until its procedure was developed in 2010. A CIP-001 procedure was developed before registration date but the entity did not distribute it to their personnel until late 2010. The TRE_URE6 was using an emergency procedure that included awareness of some sabotage events with that specifically covered terrorist attacks. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the entity had a deficient procedure in place that covered potential terrorist attacks. The procedure did include an FBI phone number but did not include reporting procedures. Texas RE also considered the size of the entity and its impact on the system. The entity is responsible for a small amount of generation on its system. | The current procedures address the requirements of CIP-001 and personnel were trained on current procedure. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 7 (TRE_URE7)Victoria Electric Cooperative, INC. (Victoria Electric Cooperative) | NCRXXXXX | TRE201100362 | CIP-001-1 | R1 | As a result of an Audit, Texas RE determined that the TRE_URE7 failed to have procedures in effect for compliance to CIP-001-1 R1, R2 and R3 from when it was registered until its operations personnel were trained in their new sabotage awareness procedure.<br>The previous emergency response plan did not explicitly contain a procedure for recognition of sabotage events or explicitly contain steps to make operating personnel aware of sabotage events. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the TRE_URE7 does not own any BES equipment, transmission lines, substations, UFLS, UVLS, or SPS equipment. | The Entity's current procedure addresses the requirements of CIP-001 and TRE_URE7's personnel have been trained on the current procedure. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 7 (TRE_URE7)Victoria Electric Cooperative, INC. (Victoria Electric Cooperative) | NCRXXXXX | TRE201100363 | CIP-001-1 | R2 | As a result of an Audit, Texas RE determined that the TRE_URE7 failed to have procedures in effect for compliance to CIP-001-1 R1, R2 and R3 from when it was registered until its operations personnel were trained in their new sabotage awareness procedure.<br>The previous emergency response plan did not explicitly contain a procedure concerning sabotage events but it did provide procedures to communicate information to appropriate parties in the Interconnection during an emergency. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the TRE_URE7 does not own any BES equipment, transmission lines, substations, UFLS, UVLS, or SPS equipment. | The Entity's current procedure addresses the requirements CIP-001 and its personnel have been trained on the current procedure. |
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 7 (TRE_URE7)Victoria Electric Cooperative, INC. (Victoria Electric Cooperative) | NCRXXXXX | TRE201100364 | CIP-001-1 | R3 | As a result of an Audit, Texas RE determined that the TRE_URE7 failed to have procedures in effect for compliance to CIP-001-1 R1, R2 and R3 from when it was registered until its operations personnel were trained in their new sabotage awareness procedure.<br>The previous emergency response plan did not explicitly provide for sabotage response guidelines but it did include emergency response guidelines and personnel to contact for reporting emergencies. | This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because the TRE_URE7 does not own any BES equipment, transmission lines, substations, UFLS, UVLS, or SPS equipment. | The Entity's current procedure addresses the requirements CIP-001 and its personnel have been trained on the current procedure. This was verified during the audit. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Texas Regional Entity, Inc. (Texas RE) | Unidentified Registered Entity 8 (TRE_URE8) | NCRXXXXX | TRE201100241 | CIP-004-2 | R2.2.4 | During a Spot-Check, Texas RE reviewed a training presentation and determined that TRE_URE8's training program for personnel did not include actions plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. TRE_URE8 revised its training to include these actions plans and procedures to address the requirements of R2.2.4. This training was implemented once the last employee with CCA access received the training, which records indicate was early in 2011. | This issue did not pose a serious or substantial risk and posed a minimal actual risk and a moderate potential risk to the bulk power system because the entity had procedures in place that included action plans and procedures to recover or re-establish CCAs and access to CCAs but lacked personnel training on these procedures. The actual risk was minimal because an event triggering the use of procedures to recover or re-establish Critical Cyber Assets never occurred during the non-compliance period. | TRE_URE8 fixed its training program almost immediately following the discovery of the deficiency which was during their Certification. Employees were trained on the action plans and procedures to recover CCAs following a cyber-security incident. |
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 1 (WECC_URE1) | NCRXXXXX | WECC201002405 | CIP-004-2 | R4 | WECC_URE1 self-reported to WECC that it did not revoke access within 7 days for an employee working for a different entity at a co-owned facility who was terminated in good standing. The employee worked for a different entity in a co-owned facility, and the employer took possession of the employee's ID badge and substation card key. The employer did not notify WECC_URE1 until two months after the last day of employment, at which time WECC_URE1 revoked access and updated its access list. The co-owner did not notify WECC_URE1 until September 2010, during a quarterly update, that it revoked access for this employee. WECC_URE1 immediately updated its access list at that point, however, the employee's last day at the co-owned facility was July 9, 2010. | This issue posed a minimal and not serious or substantial risk to the bulk power system. Although WECC_URE1 did not revoke access, the employee involved with this issue worked for a separate employer. The employee's company promptly revoked access the same day the employee left the company. Specifically, the employer physically took possession of the employee's access card and substation card key. Therefore the employee had no means to access the substation, and the employee did not otherwise have electronic or physical access rights to Critical Cyber Assets.<br><br>The entity has demonstrated a strong compliance culture demonstrated through prompt self-reporting, cooperation and collaboration in compliance matters, extensive mitigating measures when involved in compliance matters and steps to prevent recurrence. | The co-owner notified WECC_URE1 which updated its access list, disabled the employee's ID card (which, as described above, was in the possession of the company, not the employee), and verified that that ID card had not been used since the employee's last day at the co-owned facility. |
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 2 (WECC_URE2) | NCRXXXXX | WECC201102740 | CIP-004-1 | R3 | WECC_URE2 self-reported to WECC that a contractor was listed as completing a criminal background check on December 9, 2008 instead of the correct date December 9, 2002. WECC_URE2 reported that it failed to revoke access on December 9, 2009, the date on which the contractors Criminal background check performed on December 9, 2002 expired. WECC_URE2 detected this issue on January 17, 2011 during a review of personnel records, which indicated that the contractor's last background check was performed on December 9, 2002 and not December 9, 2008. | This issue posed a minimal and not serious or substantial risk to the bulk power system because the violation is limited to a single individual with access rights to one physical security perimeter (PSP) containing two Critical Cyber Assets which the contractor did not access at any time during the issue period of December 9, 2009 through January 17, 2011. Further, as represented by the individual's background check expiring, the individual was a long-time contractor in good standing at WECC_URE2. | Access was revoked for the contractor. To avoid similar instances of noncompliance in the future, WECC_URE2 created a database that links to Human Resources records and does not require manual entry or review of personnel records. The database includes a reporting functionality and appropriate WECC_URE2 staff have completed CIP-004 retraining. Further, Personnel Risk Assessment reviews are now reviewed by Security personnel as well as Information Technology. |
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 3 (WECC_URE3) | NCRXXXXX | WECC201002322 | CIP-007-1 | R5 | A CIP Spot Check of WECC_URE3's parent company's facilities including WECC_URE3. During the course of Subject Matter Expert interviews at the WECC_URE3 control center, it was discovered that WECC_URE3 had not changed the shared Energy Management System (EMS) operator account when personnel changes had occurred. At the Audit, WECC_URE3 did not demonstrate how the EMS shared account at the operating system level on operator consoles has been changed following personnel changes.<br><br>In 2009 the job status changed for two WECC_URE3 employees with EMS administrative account access such that they no longer needed access to the EMS administrative account. One employee with EMS administrative account access transferred to a different role within the company on August 31, 2009. The other employee with EMS administrative account access retired on December 31, 2009. Neither of these employees had RSA capability. However, the shared passwords for the WECC_URE3 EMS administrative account were not changed within 7 days of these changes in job status as required by the Company's policy; rather, the shared password was changed on July 1, 2010.<br><br>The issue arose because of a gap between the requirements of the company policy and the specific procedure to implement the policy. The detailed implementing procedure in effect at the time did not contain express instructions to manage the modifications for shared account access. In this instance, although WECC_URE3 had a policy for managing shared accounts, a shared EMS account password was not changed within 7 days of 2 personnel no longer requiring access to the account. | This issue posed a minimal and not serious or substantial risk to the bulk power system. While failure to establish technical and procedural controls to authenticate and account for user activity for system access could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets and such access may then be used to cause harm to Critical Cyber Assets essential to the operation of the BPS, in this instance, physical access to the facilities containing the EMS was removed within 1 day of the access change for these personnel and those personnel did not have remote cyber access into the EMS. WECC_URE3 had 24x7 monitoring of logs and alerts, physical controls per CIP-006 in place at the facilities in scope, and the personnel in scope had current Personnel Risk Assessments and current CIP training. | WECC_URE3 revised/replaced the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment; changed the two shared account passwords identified as part of the Spot Check; corrected all shared accounts discovered to be non-compliant, where doing so does not pose unacceptable adverse impacts; completed the investigation and verification for shared password accounts in the CIP environment; completed the review and updating of policies, processes, and procedures to reflect accurate and up to date controls that comply with CIP-007 R5; communicated and trained administrators on any changes to the processes and procedures and comply with CIP-007 R5; and considered and evaluated longer-term solutions to improve the management of shared password accounts within the CIP environment. |
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 4 (WECC_URE4) City of Roseville (CYRO) | NCRXXXXX | WECC201102759 | CIP-003-3 | R2 | WECC_URE4 self-certified that it had failed to document a successor to the senior manager with CIP responsibilities within 30 days of the senior manager's retirement. The previous WECC_URE4 CIP senior manager retired on December 23, 2010, WECC_URE4 assigned the successor the same day the previous CIP senior manager retired. | This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system because WECC_URE4 did install a new senior manager; the failure was only in the lack of documentation. The WECC_URE4 CIP senior manager role was continually filled with no gaps, however WECC_URE4 did not document when the previous CIP senior manager retired and the new CIP senior manager assumed the role. There was no lag or gap in CIP oversight. Further, WECC_URE4 does not have Critical Cyber Assets. | WECC_URE4 implemented the process by effectively replacing the previous CIP senior manager in a timely manner without any lapse in CIP senior manager Responsibilities and documenting the new CIP senior manager. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 5 (WECC_URE5) | NCRXXXXX | WECC2010002668 | CIP-006-1 | R1 | WECC_URE5 self-certified that it failed to provide continuous escorted access to an individual inside a Physical Security Perimeter (PSP). While in the PSP, the escort left the individual being escorted for 30 seconds to receive a package. | This issue posed minimal and not serious or substantial risk to the bulk power system because the person being escorted was not an extended distance for the escort. Further, the escort is a long-term employee in good standing and the visitor was a family member visiting the employee.<br><br>The entity has demonstrated a strong compliance culture demonstrated through prompt self-reporting, cooperation and collaboration in compliance matters, extensive mitigating measures when involved in compliance matters and steps to prevent recurrence. | The entity conducted site evaluations to determine whether Cyber Assets were compromised and took disciplinary action against the employee that failed to follow the entity's CIP-006-1 R1 procedures. |
| Western Electricity Coordinating Council (WECC) | Unidentified Registered Entity 6 (WECC_URE6) | NCRXXXXX | WECC201102611 | CIP-009-1 | R4 | WECC_URE6 self-reported to WECC that while it included processes and procedures for backing up and storing information required to successfully restore Critical Cyber Assets in its recovery plan, it failed to document how it backed up certain devices. Specifically, WECC_URE6 did appropriately back-up the devices related to the issue, but WECC_URE6 did not document the back-up in accordance with WECC_URE6's documented procedure. | This issue posed a minimal and not serious or substantial risk to the bulk power system because WECC_URE6 had a process and procedure in place. WECC_URE6 implemented the process, WECC_URE6 appropriately backed up the devices such that WECC_URE6 could successfully restore or recover the devices if necessary. WECC_URE6's issue relates to how WECC_URE6 documented the back-up. WECC_URE6's internal procedures require documentation relating to backing up its devices. The referenced back up process is a sound security and cyber asset practice to ensure stability and recovery, if necessary, following a back-up.<br><br>The entity has demonstrated a strong compliance culture demonstrated through prompt self-reporting, cooperation and collaboration in compliance matters, extensive mitigating measures when involved in compliance matters and steps to prevent recurrence. | WECC_URE6 documented the back-up process. |