Federal Energy Regulatory Commission
Washington, D.C. 20426
December 23, 2021

Re: FOIA No. FY19-30 (RC12-16)
Forty First 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 November 23, 2021, 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. RC12-16, along with the names of two (2) relevant UREs inserted on the first page, 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 RC12-16.

With respect to the remaining identities of UREs contained in RC12-16, 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

[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 staff initially determined that disclosure of identities may be appropriate.

whether there is a Technical Feasibility Exception involved that does not allow the 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 RC12-16 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: 2021.12.23 09:47:26 -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

RC12-16

Southern Company Services, Inc. - Trans (SCS-Trans)-.pdf page 18
Idaho Power Company (IPCO)-.pdf page 21

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)	Gainesville Regional Utilities (GRU)	NCR00032	FRCC2011008750	PRC-005-1	R2	On December 8, 2011, GRU, as a Generator Owner, self-reported an issue with PRC-005-1 R2. GRU has insufficient evidence to verify that generating unit batteries were maintained in accordance with GRU's generation Protection System maintenance and testing procedure for Deerhaven Units CT1, CT2 and CT3 in March and April 2010, and for Deerhaven Unit DH1 in February, March and April 2010. Deerhaven Unit DH1 was in an extended plant outage during February, March and April 2010. In addition, GRU's April 2011 monthly inspections for generating unit batteries on Deerhaven Unit DH1 were performed three days late.	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 batteries are continuously monitored and would have alarmed the control room if any issues were identified. Additionally, the batteries were visually checked each day while operators were doing rounds. Third, GRU performed quarterly and annual battery testing in accordance with its procedures. Lastly, documentation is missing for only three months of monthly battery testing, with respect to the 2010 maintenance, or is late by only three days, in the case of the April 2011 inspections. Although GRU violated this Standard on two prior occasions and had one prior remediated issue with this Standard, FRCC determined that the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation. Two of the prior instances involved relays and one involved relays and battery maintenance on transmission batteries. Following the prior violations, all of which were mitigated by August 2010, GRU made changes to its preventative maintenance software to ensure that batteries were tested according to the intervals defined in its Protection System maintenance and testing program, and improved its procedures for keeping and reviewing documentation of maintenance and testing. Those improvements, however, did not explicitly address maintenance of battery banks during plant outages, which is at issue here with respect to GRU's Unit DH1.	To mitigate this issue, GRU tested and maintained the batteries that were out of interval and in addition, revised its generation Protection System maintenance and testing procedure to address testing of batteries during plant outages. FRCC has verified completion of the mitigation activities.
Reliability*First* Corporation (Reliability*First*)	Northern Indiana Public Service Company [DP GO GOP LSE PSE RP TP] (NIPSCO)	NCR02610	RFC2012010007	FAC-008-1	R1	From December 6, 2011 through December 13, 2011, Reliability*First* conducted a compliance audit of NIPSCO (Audit). During the Audit, Reliability*First* determined NIPSCO, as a Generator Owner, did not document the methodology it used to determine the Facility Ratings for current transformers (CTs), a relay protective device, on its Bailey Unit 7 generating unit (Unit 7). Reliability*First* discovered that NIPSCO does not have a unified document describing the methodologies used to determine ratings for equipment on its generators. Rather, NIPSCO created separate documents for each generator consisting of a table that lists the method for determining the Facility Ratings for the associated equipment. Reliability*First* determined that NIPSCO had an issue with FAC-008-1 R1 for failing to document the methodology for determining Facility Ratings for CTs on the table associated with Unit 7.	Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated because the issue is an isolated documentation error. It is an isolated documentation error that does not indicate a systemic problem because NIPSCO had a Facility Rating for its CTs at Unit 7 during the duration of the issue but neglected to document the methodology it used to determine the Facility Rating on Unit 7's associated table. NIPSCO based the Facility Ratings for all generating unit CTs, including Unit 7's CTs, on manufacturer's recommendations and nameplate ratings. NIPSCO documented this methodology on the associated tables of each generating unit except that of Unit 7.	NIPSCO documented the methodology it used to determine the Facility Rating for its Unit 7 CTs.
Reliability*First* Corporation (Reliability*First*)	Northern Indiana Public Service Company [TO TOP BA] (NIPSCO)	NCR02611	RFC2012010017	PER-002-0	R3	From December 6, 2011 through December 13, 2011, Reliability*First* conducted a compliance audit of NIPSCO (Audit). During the Audit, Reliability*First* determined NIPSCO, as a Balancing Authority and Transmission Operator, did not document Regional Reliability Organization standards, entity operating procedures, and applicable regulatory requirements as objectives in its training program pursuant to PER-002-0 R3.1. NIPSCO did include NERC certification as an objective in its training program. Additionally, Reliability*First* determined NIPSCO did not adequately identify its training staff in its training program pursuant to PER-002-0 R3.4.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated because this was a documentation error. It was a documentation error because the issue relates to the lack of documentation of objectives and identification of trainers in the training program. Reliability*First* did not find that the training materials failed to address the objectives described in PER-002-0 R3.1. Additionally, Reliability*First* did not find the adequacy of the training staff was insufficient. During the Audit, NIPSCO submitted resumes from its training staff demonstrating the staff's variety of tenure and industry experience. Additionally, all NIPSCO training staff had completed Midwest ISO's "Train-the-Trainer" series prior to the issue.	NIPSCO updated its training program to include documentation of all the objectives and identified its training staff as required by PER-002-0 R3.1 and R3.4.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Sunbury Generation LP (Sunbury)	NCR06030	RFC2012010025	VAR-002-1.1b	R3	On April 3, 2012, Sunbury self-reported an issue with VAR-002-1.1b R3 to Reliability*First* . Sunbury reported that, as a Generator Operator, on March 24, 2012, it experienced a status change on one of its generating units but did not notify its Transmission Operator (TOP) until 32 minutes after the status change, instead of within 30 minutes as required by the Standard. Prior to March 24, 2012, all of Sunbury's generating units were shut down for economic reasons. Subsequently, Sunbury's TOP requested Sunbury to start its Unit 1 generator to provide reactive support on a day-by-day basis while the local Transmission Owner completed maintenance and upgrade work. Sunbury did so with only one plant control operator operating its Unit 1 generator, a reduced operating staff relative to Sunbury's normal operations. On March 24, 2012, the Unit 1 generator tripped due to a relay operation, which caused the automatic voltage regulator (AVR) to trip into manual mode. Due to the staffing shortages and the economic shutdown status, there was one operator on duty at the time. Under normal operating conditions, another operator would have been on duty as well. The operator responded to the trip event and did not notify the TOP of the status change on the AVR until 32 minutes after generating Unit 1 was returned to service with the AVR in manual mode.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Sunbury's generator was operating at its minimum load level (40 MW) at the time of the trip. In addition, Sunbury's two minute delay in notifying its TOP was caused by unusual staffing conditions related to the fact that Sunbury was shut down for economic reasons. Finally, Sunbury notified its TOP of this status change two minutes after the expiration of the 30-minute notification requirement of VAR-002-1.1b R3.	To mitigate this issue, Sunbury reviewed the requirements of VAR-002-1.1b with the shift supervisors, who are available and on duty during the shutdown periods and during periods of limited operation. During these reviews, Sunbury emphasized the 30-minute notification requirement. In addition, Sunbury placed notifications at each of the station's AVR control locations to remind the operators of the 30-minute notification requirement.
Reliability*First* Corporation (Reliability*First*)	ITC Transmission (ITCT)	NCR00803	RFC2012001324	FAC-009-1	R1	From August 15, 2011 through August 23, 2011, Reliability*First* conducted a compliance audit of ITCT and its affiliate entity, METC (Audit). During the Audit, Reliability*First* discovered that METC had an issue with FAC-009-1 R1. Subsequently, ITCT determined that there was an additional instance of this issue that implicated ITCT, as a Transmission Owner. ITCT failed to revise the Facility Ratings for three transformers pursuant to its revised Facility Ratings Methodology, in effect as of March 16, 2010. Specifically, one of ITCT's 345/120 kV transformers had Facility Ratings higher than those required by the Facility Ratings Methodology. This transformer was consistent with the Facility Ratings Methodology in place prior to March 16, 2010. However, ITCT failed to revise the Ratings for this transformer after the effective date of its revised Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The transformer has a remote monitoring system that captures real-time values and that alarms for hot spot and top oil temperatures as well as fault gasses. Thus, if a fault occurred, ITCT could monitor and evaluate these critical parameters to ensure the transformer was not unsafely operating. In addition, the transformers at issue constitute less than 3% of ITCT's solely and jointly owned facilities. In addition, during the time the incorrect Facility Ratings were in effect, transformer loading did not exceed the correct Facility Rating. In addition, the respective summer and winter normal ratings for that transformer decreased by only 1.25% and 2.3%. For the ITCT transformer, when the Normal Facility Rating decreased after ITCT applied its revised Facility Ratings Methodology, ITCT increased the winter emergency rating for that transformer, illustrating that the previous lower Facility Rating was not endangering the operability of that transformer.	ITCT committed to take the following actions to address the issue with FAC-009-1 R1. ITCT issued revised Facility Ratings for ITCT's St. Clair PP #306 345/120 kV transformer.
Reliability*First* Corporation (Reliability*First*)	METC	NCR00820	RFC2011001174	FAC-009-1	R1	From August 15, 2011 through August 23, 2011, Reliability*First* conducted a compliance audit of METC and its affiliate entity, ITC Transmission, during which Reliability*First* discovered that METC had an issue with FAC-009-1 R1 (Audit). METC failed to revise the Facility Ratings for three transformers pursuant to their revised Facility Ratings Methodology, in effect beginning March 16, 2010. Specifically, two of METC's 345/138 kV transformers had Facility Ratings higher than those required by the Facility Ratings Methodology. These transformers were consistent with the Facility Ratings Methodology in place prior to March 16, 2010. However, METC failed to revise the Ratings for these transformers after the effective date of their revised Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. All transformers have a remote monitoring system that captures real-time values and that alarms for hot spot and top oil temperatures as well as fault gases. Thus, if a fault occurred, METC could monitor and evaluate these critical parameters to ensure the transformer was not unsafely operating. In addition, the transformers at issue constitute less than 3% of METC's solely and jointly owned facilities. In addition, during the time the incorrect Facility Ratings were in effect, transformer loading did not exceed the correct Facility Rating. For one of the METC transformers, METC was required to revise the Facility Rating after applying its revised Facility Ratings Methodology as a conservative measure to prolong the life of the transformer. The transformer's capability did not change. For the other METC transformer, when the Normal Facility Rating decreased after METC applied its revised Facility Ratings Methodology, METC increased the Emergency Rating for that transformer, illustrating that the previous lower Facility Rating was not endangering the operability of that transformer. In addition, the respective summer and winter normal ratings for that transformer decreased by only 1.25% and 2.3%.	METC committed to take the following actions to address the issue with FAC-009-1 R1. METC issued revised Facility Ratings for METC's Tallmadge #2 345/138 kV transformer and Tallmadge #3 345/138 kV transformer.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	PPL - Lower Mount Bethel Energy, LLC (LMBE)	NCR00882	RFC2011001193	FAC-008-1	R1	From September 12, 2011 through September 30, 2011, Reliability*First* conducted a compliance audit of LMBE and its affiliate entity, PPL Holtwood, L.L.C (Audit). During the Audit, Reliability*First* discovered that LMBE, as a Generator Owner, had an issue with FAC-008-1 R1. LMBE has in place Facility Ratings Methodologies pursuant to FAC-008-1 R1. LMBE's three generating units interconnect with PPL EU at 230 kV through a generator step-up transformer (GSU). Pursuant to an Interconnection Agreement, the transition of ownership of the transmission conductors between LMBE and its Transmission Owner, PPL Electric Utilities Corporation, at its interconnection point occurs above the fence where the transmission conductors enter the 230 kV switchyard, which is mid-span. Thus, LMBE owns less than one mile of transmission line from GSU to the interconnection point. LMBE; however, failed to include the method by which it determines the Facility Rating for these transmission conductors in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The Transmission Owner had a facility Rating for each transmission conductor and operated its side of the transmission conductors within that Facility Rating. In addition, LMBE generating stations were designed such that the generator is the most limiting element. As a result, these short spans of interconnecting conductors owned by LMBE are less likely to limit the generating station's capacity.	LMBE reviewed the Facility Ratings of these conductors not including in its Facility Rating matrices and confirmed that these ratings were not the most limiting for the Facility. On January 24, 2012, LMBE issued updated Facility Ratings matrices that included the equipment ratings and methodology.
ReliabilityFirst Corporation (ReliabilityFirst)	PPL Holtwood, L.L.C. (PPL Holtwood)	NCR00886	RFC2011001198	FAC-008-1	R1	From September 12, 2011 through September 30, 2011, Reliability*First* conducted a compliance audit of PPL Holtwood and its affiliate entity, PPL - Lower Mount Bethel Energy, LLC (Audit). During the Audit, Reliability*First* discovered that PPL Holtwood, as a Generator Owner, had an issue with FAC-008-1 R1. PPL Holtwood has in place Facility Ratings Methodologies pursuant to FAC-008-1 R1. PPL's Holtwood's ten generating units interconnect at two points with PPL EU at 60 kV through three generator step-up transformers (GSU). Pursuant to an interconnection agreement, the ownership transition between PPL Holtwood and its Transmission Owner, PPL Electric Utilities Corporation, occurs at the disconnect switch on the high voltage side of the GSU, its interconnection point. Thus, PPL Holtwood owns the conductors between the GSU and the high voltage disconnect switch. The distance between each of the GSUs and its respective disconnect switch is between approximately ten and 25 feet. PPL Holtwood, however, failed to include the method by which it determines the Facility Ratings for these transmission conductors in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The Transmission Owner had a facility Rating for each transmission conductor and operated its side of the transmission conductors within that Facility Rating. In addition, PPL Holtwood generating stations were designed such that the generator is the most limiting element. As a result, these short spans of interconnecting conductors owned by PPL Holtwood are less likely to limit the generating station's capacity.	PPL Holtwood reviewed the Facility Ratings of these conductors not including in its Facility Rating matrices and confirmed that these ratings were not the most limiting for the Facility. On January 24, 2012, PPL Holtwood issued updated Facility Ratings matrices that included the equipment ratings and methodology.
SERC Reliability Corporation (SERC)	Entergy	NCR01234	SERC2011007395	VAR-002-1.1a	R3	On June 8, 2011, Entergy, as a Generator Operator (GOP), self-reported an issue of VAR-002-1.1a R3 because it could not find evidence that an automatic voltage regulator (AVR) status change on August 16, 2010, had been reported to the Transmission Operator (TOP) within 30 minutes, as required. According to a timestamp-plot provided by Entergy, on August 16, 2010, station service power was lost for nine minutes and nine seconds. Entergy indicated that while the AVR was back in automatic voltage control mode within 10 to 15 minutes following the loss of power, notification to the TOP was never provided.	SERC staff 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: 1. At the time of this occurrence, three units were online, generating 125 MW (100% capacity), 500 MW (79% capacity), and 740 MW (100% capacity), respectively. The contribution of the unit at issue to voltage control was a small fraction of the station's capability; 2. At the time of this occurrence, Entergy's operator was aware of the condition, controlling the voltage manually and in the process of restoring the AVR.	SERC staff verified that Entergy completed the following actions: 1. Held a meeting with applicable personnel to discuss the VAR-002 procedure, the event and lessons learned; and 2. Installed signs in the vicinity of all of the AVR controls that remind personnel of the VAR-002 notification requirements.
SERC Reliability Corporation (SERC)	Entergy	NCR01234	SERC2011007432	VAR-002-1.1a	R1	On June 14, 2011, Entergy, as a Generator Operator (GOP), self-reported an issue of VAR-002-1.1a R1 because on August 16, 2010, a station service transformer breaker tripped causing the automatic voltage regulator (AVR) to switch from automatic voltage control mode to manual mode and notification to the Transmission Operator (TOP) had not been given, as required. According to a timestamp-plot provided by Entergy, on August 16, 2010, station service power was lost for 9 minutes and 9 seconds. Entergy indicated that the AVR was back in automatic voltage control mode within 10 to 15 minutes following the loss of power. However, notification to the TOP had not been provided prior to the AVR switching to manual mode.	SERC staff 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: 1. At the time of this occurrence, three units were on line each generating 125 MW (100% capacity), 500 MW (79% capacity), and 740 MW (100% capacity), respectively. The contribution of the unit at issue to voltage control was a small fraction of the station's capability; and, 2. At the time of this occurrence, Entergy's operator was aware of the condition, controlling the voltage manually and in the process of restoring the AVR to automatic voltage control mode.	SERC staff verified that Entergy completed the following actions: 1. Held a meeting with applicable personnel to discuss the VAR-002 procedure, the event and lessons learned; 2. Installed signs in the vicinity of all of the AVR controls that remind personnel of the VAR-002 notification requirements.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Tenaska Virginia Partners, L.P. (TVP)	NCR01339	SERC2011007877	VAR-002-1.1b	R3	On August 12, 2011, TVP, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3, stating that on June 13, 2011, when the plant resumed operation following an outage, the TVP operator was not aware that the power system stabilizer (PSS) associated with its steam turbine generator had changed its status to disabled. As a result, TVP did not report this status change to its Transmission Operator (TOP). On June 28, 2011, when TVP became aware that the PSS was disabled, TVP immediately enabled it but notified the TOP outside of the 30-minute time limit required by VAR-002-1.1b R3. TVP operates a combined-cycle generating station with a rating of approximately 885 MW. The station consists of three combustion turbine generators (CTGs) with a combined rating of approximately 495 MW and a steam turbine generator (STG) rated at approximately 390 MW. TVP shut down its STG unit for maintenance between April 2, 2011 and June 13, 2011. During this period, the STG excitation system was powered down. As TVP ended the outage, it powered up the STG excitation system to support the STG coming online. As a result of its default control logic, the PSS was disabled while the excitation system was powered up. The PSS remained disabled until June 28, 2011, when TVP discovered the issue following TVP internal compliance review efforts. TVP re-enabled the PSS at 10:18 A.M., but did not notify the TOP until 11:55 A.M. SERC learned that although TVP included checking the “PSS Enabled” field in the CTG startup checklist, this step was not included in the STG startup checklist.	SERC staff 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: 1. TVP was able to maintain system voltage in accordance with the TOP voltage schedule; 2. All three CTGs were operating with PSS in service during the time that the STG was operating without the PSS in service, which would help control the system voltage; and 3. The TOP confirmed that a small voltage excursion by TVP would have little impact on overall grid voltage and other plants in the area could easily compensate for such an excursion.	SERC staff verified that TVP completed the following actions: 1. Added a control system alarm that will alert personnel when the PSS status changes from disabled to enabled to remind the operator of the 30 minute reporting requirement. This alarm will remain visible for one hour after the change in status to minimize locked-in alarms; 2. Added a control system alarm that will alert personnel when the PSS status changes from enabled to disabled. This alarm will re-annunciate every day at 8:00 A.M., as operation with the PSS disabled is not a normal condition and warrants a daily reminder; 3. Added a pop-up window to remind the control room operator of NERC requirements for notifying the TOP when the status of the PSS changes; 4. Changed the default control logic for the PSS while the unit powers up to enabled; 5. Created a quick reference document to be kept in the control room operator reference book listing all applicable reporting requirements that include a time restriction; and 6. Conducted monthly plant training that included a review of TVP's internal compliance review comments, refresher training on NERC reporting requirements, and refresher training on PSS operations.
Southwest Power Pool Regional Entity (SPP RE)	Cleco Corporation (Cleco)	NCR01083	SPP2012010777	VAR-002-1.1b	R3	On July 26, 2012, Cleco, as a Generator Operator, self-reported a possible remediated issue of VAR-002-1.1b R3 for failing to notify its Transmission Operator (TOP) of a status change on a generator’s automatic voltage regulator (AVR) within 30 minutes. On May 12, 2012, Cleco’s Teche Unit #3 AVR tripped to manual mode, but was immediately reset to automatic mode. After resetting the AVR, Cleco’s operating personnel proceeded to contact its TOP via its Generation Ops database; however, the database was down. Cleco’s operating personnel managed to contact its TOP and inform the TOP of the status change of the AVR within 33 minutes and 8 seconds after the change occurred.	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 Cleco’s AVR trip was momentary and Cleco’s system operators immediately reset the AVR to automatic mode. Additionally, Cleco was late only 3 minutes and 8 seconds over the required time to contact its TOP and report the AVR status change.	Cleco added an alarm point to its supervisory control and data acquisition (SCADA) system for the AVR at Teche Unit # 3. This alarm was fully tested and placed in service on May 29, 2012. The alarm point will provide a backup to the normal notification process. In addition, Cleco’s NERC Compliance & Training department completed the Power Plant NERC training at Teche Unit #3 on July 26, 2012. This training was mandatory for all operating personnel at Teche Unit #3. The training included a review of VAR-002 plus COM-002, CIP-001, PRC-001 and EOP-005.
Southwest Power Pool Regional Entity (SPP RE)	Midwest Energy, Inc. (Midwest)	NCR01118	SPP2012010068	EOP-005-1	R6	On April 16, 2012, Midwest, as a Transmission Operator, self-reported a possible noncompliance with EOP-005-1 R6 because it could not substantiate that three of its system operators had participated in annual system restoration training exercises during 2011. Specifically, Midwest had one system operator who did not complete the annual restoration training required in 2011. Midwest also had two system operators who did receive restoration training in 2011. However, they were not certified as system operators at the time, they were not registered in the Southwest Power Pool Regional Transmission Organization's (SPP RTO) Learning Management System (LMS), which would have documented their training.	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 one of Midwest’s system operators did not participate in annual system restoration training in 2011, he had participated in SPP RTO regional restoration drills in 2009 and 2010. Furthermore, he had completed 32 hours of emergency operations training from other training resources. As to the remaining two system operators, they participated in the SPP RTO sponsored restoration training in 2011; however, because they were not certified as system operators at the time of training, their participation was not formally documented in Midwest's LMS.	Midwest provided the system operators at issue emergency operations training on restoration of the Midwest's system. Additionally, all system operators are now required to register in the SPP RTO's LMS for all SPP RTO training in which they participate to ensure documentation of the training, regardless of system operator certification status at the time of the training.
Southwest Power Pool Regional Entity (SPP RE)	The Empire District Electric Company (EDE)	NCR01155	SPP201000338	PRC-005-1	R2.1	On July 27, 2010, EDE submitted a Self-Report stating that it had possible noncompliance with PRC-005-1 R2.1 because it failed to inspect five station batteries at two of its substations within the ninety day period prescribed by its Protection Systems devices testing and maintenance plan. The two substations reported were Decatur South #392 and Neosho South Junction #184. EDE owns or controls 4,787 Protection System devices. EDE inspected the batteries at these two substations on March 10, 2010, but did not inspect them again until July 1, 2010 and July 12, 2010 respectively. This remediated issue is applicable to EDE's Transmission Owner, Generator Owner and Distribution Provider functions.	SPP RE 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 of the limited scope and duration of this remediated issue. The scope of the issue was the failure to perform quarterly battery inspections on five batteries at two substations. Battery inspections at the two substations were performed on March 10, 2010 and were due to be performed again on or before June 8, 2010. EDE discovered the oversight and tested the batteries on July 1, 2010 and July 12, 2010.	EDE performed the inspections of the five batteries located in its Decatur South #392 and Neosho South Junction #184.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	EnerNOC, Inc. (EnerNOC)	NCR11021	TRE2012009969	CIP-001-1	R1	During an Audit that ended March 30, 2012, Texas RE, discovered that EnerNOC, as a Load Serving Entity (LSE), had a remediated issue of CIP-001-1 R1. EnerNOC is a demand response provider in the Electric Reliability Council of Texas (ERCOT) service territory. The EnerNOC's security plans (Crisis Management Plan, Business Contingency Plans, Disaster Recovery procedures and Computer Security Incident Response Team) did not have a definition of sabotage events or include 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. EnerNOC was non-compliant with this Standard from April 12, 2010, the date of its registration as a LSE, through March 26, 2012, the date the revised sabotage event plans and procedures were completed.	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 EnerNOC already had existing procedures to address and handle cyber and physical emergency events and because of EnerNOC 's size. EnerNOC's largest emergency interruptible load service in this region is 12.8 MW and its maximum total capability of demand response is 150 MW. In addition, the EnerNOC does not have large physical structures or facilities that are interconnected to the grid and that are susceptible to sabotage, thereby reducing the risk to the BPS. The risk was also mitigated by the fact that EnerNOC provides its services through multiple data centers and dispatch centers and is therefore less vulnerable to cyber attacks.	EnerNOC's emergency plans were updated to address the requirement of this Standard before the conclusion of the Audit. Mitigation included development and approval of EnerNOC's revised "ERCOT Contingency Protocol," communication of the revised procedures to personnel, and incorporation of the revised documentation into EnerNOC's document management system. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	EnerNOC, Inc. (EnerNOC)	NCR11021	TRE2012009970	CIP-001-1	R2	During an Audit that ended March 30, 2012, Texas RE, discovered that EnerNOC, as a Load Serving Entity (LSE), had a remediated issue of CIP-001-1 R2. EnerNOC is a demand response provider in the Electric Reliability Council of Texas (ERCOT) service territory. EnerNOC's security plans (Crisis Management Plan, Business Contingency Plans, Disaster Recovery procedures and Computer Security Incident Response Team) did not have a definition of sabotage events or have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. EnerNOC was non-compliant with this Standard from April 12, 2010, the date of its registration as a LSE, through March 26, 2012, the date it revised its plans and procedures.	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 EnerNOC already had existing procedures to address and handle cyber and physical emergency events and because of EnerNOC 's size. EnerNOC's largest emergency interruptible load service in this region is 12.8 MW and its maximum total capability of demand response is 150 MW. In addition, the EnerNOC does not have large physical structures or facilities that are interconnected to the grid and that are susceptible to sabotage, thereby reducing the risk to the BPS. The risk was also mitigated by the fact that EnerNOC provides its services through multiple data centers and dispatch centers and is therefore less vulnerable to cyber attacks.	EnerNOC's emergency plans were updated to address the requirement of this Standard before the conclusion of the Audit. Mitigation included development and approval of EnerNOC's revised "ERCOT Contingency Protocol," communication of the revised procedures to personnel, and incorporation of the revised documentation into EnerNOC's document management system. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	EnerNOC, Inc. (EnerNOC)	NCR11021	TRE2012009971	CIP-001-1	R3	During an Audit that ended March 30, 2012, Texas RE, discovered that EnerNOC, as a Load Serving Entity (LSE), had a remediated issue of CIP-001-1 R2. EnerNOC is a demand response provider in the Electric Reliability Council of Texas (ERCOT) service territory. EnerNOC's security plans (Crisis Management Plan, Business Contingency Plans, Disaster Recovery procedures and Computer Security Incident Response Team) did not have a definition of sabotage events or provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events. EnerNOC was non-compliant with this Standard from April 12, 2010, the date of its registration as a LSE, through March 26, 2012, the date it revised its plans and procedures.	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 EnerNOC already had existing procedures to address and handle cyber and physical emergency events and because of EnerNOC 's size. EnerNOC's largest emergency interruptible load service in this region is 12.8 MW and its maximum total capability of demand response is 150 MW. In addition, the EnerNOC does not have large physical structures or facilities that are interconnected to the grid and that are susceptible to sabotage, thereby reducing the risk to the BPS. The risk was also mitigated by the fact that EnerNOC provides its services through multiple data centers and dispatch centers and is therefore less vulnerable to cyber attacks.	EnerNOC's emergency plans were updated to address the requirement of this Standard before the conclusion of the Audit. Mitigation included development and approval of EnerNOC's revised "ERCOT Contingency Protocol," communication of the revised procedures to personnel, and incorporation of the revised documentation into EnerNOC's document management system. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	Sweetwater Wind 2 LLC (Sweetwater 2)	NCR04132	TRE201100503	PRC-005-1	R1	During an April 8, 2011 Audit, Texas RE discovered that Sweetwater 2, as a Generator Owner (GO), did not have a documented generation Protection System maintenance and testing program in place, as required by PRC-005-1 R1. Sweetwater 2 is a wind generator within the Electric Reliability Council of Texas (ERCOT) service territory. Sweetwater 2 was non-compliant with this Standard from June 28, 2007, the date of its registration as a GO, to October 3, 2007, when it created a Protection System maintenance and testing program.	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: a) Sweetwater 2 has 91 MW of nameplate capacity; b) the instantaneous capability of the facility is dynamic and subject to the prevailing wind. When operating below nameplate capacity, the facility is not normally deemed to contribute operating reserves to the ERCOT system due to the uncertainties inherent in a wind resource; c) the generation Protection System was monitored 24/7 by Sweetwater 2's control center; d) during the pendency of this remediated issue, Sweetwater 2 had an Operations and Maintenance contract with General Electric, which performed Protection System maintenance and testing on the facility more often than the maintenance and testing intervals adopted by Sweetwater 2 in its PRC-005-1 R1 program adopted after October 3, 2007. GE performed relay maintenance and testing every year; e) the period of this remediated issue was three months; f) there were no relay misoperations during this period; g) there are at least two levels of overlapping protection during the pendency of this issue. Each feeder and wind turbine had protective relays; and h) Sweetwater 2 conducted weekly visual inspections.	On October 3, 2007, approximately three months after registration, Sweetwater 2 created a generation Protection System maintenance and testing program. Texas RE reviewed the program during the Audit, and determined it addressed the requirements of this Standard. Texas RE verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc	Sweetwater Wind 3 LLC (Sweetwater 3)	NCR04133	TRE201100504	PRC-005-1	R1	During an April 8, 2011 Audit, Texas RE discovered that Sweetwater 3, as a Generator Owner (GO), did not have a documented generation Protection System maintenance and testing program in place, as required by PRC-005-1 R1. Sweetwater 3 is a wind generator within the Electric Reliability Council of Texas (ERCOT) service territory. Sweetwater 3 was non-compliant with this Standard from June 28, 2007, the date of its registration as a GO, to October 3, 2007, when it created a Protection System maintenance and testing program.	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: a) Sweetwater 3 has 135 MW of nameplate capacity; b) the instantaneous capability of the facility is dynamic and subject to the prevailing wind. When operating below nameplate capacity, the facility is not normally deemed to contribute operating reserves to the ERCOT system due to the uncertainties inherent in a wind resource; c) the generation Protection System was monitored 24/7 by Sweetwater 3's control center; d) during the pendency of this remediated issue, Sweetwater 3 had an Operations and Maintenance contract with General Electric, which performed protection system maintenance and testing on the facility more often than the maintenance and testing intervals adopted by Sweetwater 3 in its PRC-005-1 R1 documented program adopted October 3, 2007. GE performed relay maintenance and testing every year; e) the period of this remediated issue was three months; f) there were no relay misoperations during the period; g) there are at least two levels of overlapping protection during the pendency of this issue. Each feeder and wind turbine had protective relays and; and h) Sweetwater 3 conducted weekly visual inspections.	On October 3, 2007, approximately three months after registration, Sweetwater 3 created a generation Protection System maintenance and testing program. Texas RE reviewed the program during the Audit, and determined it addressed the requirements of this Standard. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	Sweetwater Wind 4 LLC (Sweetwater 4)	NCR04135	TRE201100505	PRC-005-1	R1	During an April 8, 2011 Audit, Texas RE discovered that Sweetwater 4, as a Generator Owner (GO), did not have a documented generation Protection System maintenance and testing program in place, as required by PRC-005-1 R1. Sweetwater 4 is a wind generator within the Electric Reliability Council of Texas (ERCOT) service territory. Sweetwater 4 was non-compliant with this Standard from June 28, 2007, the date of its registration as a GO, to October 3, 2007, when it created a Protection System maintenance and testing program.	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: a) the instantaneous capability of the facility is dynamic and subject to the prevailing wind. When operating below nameplate capacity, the facility is not normally deemed to contribute operating reserves to the ERCOT system due to the uncertainties inherent in a wind resource; b) the generation Protection System was monitored 24/7 by Sweetwater 4's control center; c) during the pendency of this remediated issue, Sweetwater 4 had an Operations and Maintenance contract with General Electric, which performed protection system maintenance and testing on the facility more often than the maintenance and testing intervals adopted by Sweetwater 4 in their PRC-005-1 R1 program adopted on October 3, 2007. GE performed relay maintenance and testing every year. d) the period of this remediated issue was three months; e) there were no relay misoperations during the period; f) there are at least two levels of overlapping protection during the pendency of this issue; Each feeder has protective relays as well as each wind turbine; and g) Sweetwater 4 conducted weekly visual inspections.	On October 3, 2007, approximately three months after registration, Sweetwater 4 created a generation Protection System maintenance and testing program. Texas RE reviewed the program during the Audit, and determined it addressed the requirements of this Standard. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	Sweetwater Wind 5, LLC (Sweetwater 5)	NCR02715	TRE201100507	FAC-008-1	R1	During an April 8, 2011 Audit, Texas RE determined that Sweetwater 5, as a registered Generator Owner (GO), did not have a documented Facility Ratings Methodology (FRM) of its solely and jointly owned Facilities, as required by FAC-008-1 R1. Sweetwater 5 is a wind generator within the Electric Reliability Council of Texas (ERCOT) service territory. Sweetwater 5 was non-compliant with this Standard from November 1, 2007, the date of its registration as a GO, to November 19, 2007, when a FRM was created.	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: a) Sweetwater 5 was aware of the actual rating of the facility. The ratings did not change after Sweetwater 5 developed and formally applied the FRM; b) Sweetwater 5 facility is a wind generation facility comprised of, and limited by, standardized wind generators. The engineering design and actual facility performance was documented as far back as January of 2007 and it was understood in the organization that the limiting element was the sum of the generator's nameplate capacities, and c) The remediated issue lasted 18 days.	On November 19, 2007, 18 days after registration, Sweetwater 5 created a FRM. Texas RE reviewed the program during the audit, and determined it was addressing the requirements of this Standard. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	Sweetwater Wind 5, LLC (Sweetwater 5)	NCR02715	TRE201100508	FAC-009-1	R1	During an April 8, 2011 Audit, Texas RE determined that Sweetwater 5, as a registered Generator Owner (GO), did not establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology (FRM). Sweetwater 5 is a wind generator within the Electric Reliability Council of Texas (ERCOT) service territory. Sweetwater 5 was non-compliant with this Standard from November 1, 2007, the date of its registration as a GO, to November 19, 2007, when the Facility Ratings were established.	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: a) Sweetwater 5 was aware of the actual Rating of the facility. The ratings did not change after Sweetwater 5 developed and formally applied the FRM and determined the Facility Ratings pursuant to its FRM; b) Sweetwater 5 facility is a wind generation facility comprised of, and limited by, standardized wind generators. The engineering design and actual facility performance was documented as far back as January of 2007 and it was understood in the organization that the limiting element was the sum of the generator nameplate capacities; and c) The remediated issue lasted 18 days.	On November 19, 2007, 18 days after registration, Sweetwater 5 established and documented Facility Ratings in accordance with its FRM. Texas RE reviewed the ratings during the audit, and determined they were addressing the requirements of this Standard. Texas RE verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc	Sweetwater Wind 5, LLC (Sweetwater 5)	NCR02715	TRE201100510	TOP-002-2	R13	During an April 8, 2011 Audit, Texas RE determined that Sweetwater 5, as a registered Generator Operator (GOP), did not perform reactive capability testing pursuant to the Electric Reliability Council of Texas's (ERCOT) Nodal Operating Guide 3.3.2.2. Texas RE determined that Sweetwater 5 had a remediated issue of TOP-002-2 R13. Sweetwater 5 was non-compliant with this Standard from November 1, 2007, the date of its registration as a GOP, until June 22, 2012, when ERCOT, as a Transmission Operator and a Balancing Authority, stated that Sweetwater 5 had "demonstrated" prospective reactive capability in response to an engineering design study conducted on April 23, 2012.	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 wind reactive capability testing was the subject of a joint settlement between ERCOT and Sweetwater 5, among several other wind generators. Sweetwater 5 had previously conducted reactive capability testing in January of 2007 and had supplied such information to ERCOT at that time, and annually thereafter. The performance characteristics of the facility did not change materially since then. The engineering design analysis that was supplied to ERCOT on April 23, 2012 as part of the joint settlement was a prospective engineering design analysis. As part of this joint settlement, Sweetwater 5 has 14 months from June 22, 2012 to implement the needed additions to its reactive capability. ERCOT stated that the engineering design served as a "demonstration of capability."	On April 23, 2012, an engineering study was performed on planned reactive capability enhancements. This study was subsequently supplied to ERCOT. On June 22, 2012, ERCOT sent Sweetwater 5 an agreement letter stating that Sweetwater 5 had "demonstrated that its affected Wind Generation Resources are capable of meeting the required reactive standard." Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc	Brazos Electric Power Co Op, Inc. (Brazos)	NCR04015	TRE201100479	EOP-008-0	R1	During a October 7, 2011 Audit, Texas RE determined that Brazos had a remediated issue with EOP-008-0 R1 R1.1 and R1.3 because Brazos failed to complete its backup control center (BUCC). Brazos relied on the construction and commissioning of the BUCC in its plans to continue reliability operations in the event its control center becomes inoperable. As a condition of its Transmission Operator (TOP) coordinated functional registration (CFR) and TOP certification, Brazos' submitted and Texas RE approved on April 26, 2010, an implementation plan which included details and milestone dates related to the construction of the BUCC. Subsequently, Brazos was certified as a TOP effective October 1, 2010. Brazos' revised implementation plan included a milestone for completion of its BUCC by August 31, 2011. Due to technical delays with the installation of the communication system at the BUCC, Brazos was unable to commission and test the BUCC until October 13, 2011. Therefore, Texas RE determined that Brazos was noncompliant with this Standard.	Texas RE 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 Brazos had an approved implementation plan, the duration between the milestone date and actual commissioning date was inconsequential to the BUCC construction undertaking. At the time of the issue, Brazos had a backup plan in case the construction of the BUCC was delayed. The backup plan consisted of an off-site control room with remote communications to the primary control center's energy management system (EMS). If either the remote communications or EMS is not functional, Brazos could maintain control via phone. Finally, it is reasonable to assume that if Brazos had requested an extension of its Mitigation Plan, Texas RE would have been granted it given the circumstances.	This issue was mitigated when Brazos fully commissioned its BUCC on October 13, 2011. Texas RE verified completion of the mitigation activities.
Western Electricity Coordinating Council (WECC)	California Department of Water Resources (CDWR)	NCR05047	WECC2012009799	FAC-001-0	R1	During the course of an onsite Audit of CDWR compliance conducted between February 14, 2012 and February 24, 2012, the WECC Audit team determined that CDWR, as a Transmission Owner, was in noncompliance with FAC-001-0 R1, R2 and R3. Specifically, the Audit team determined that CDWR failed to document, maintain, and publish facility connection requirements per FAC-001-0 R1. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Further, the Audit Team determined that CDWR failed to make documentation available to WECC, the Regional Reliability Organization (RRO), within five days of its request for documentation of facility connection requirements per FAC-001-0 R3. On February 15, 2012, the Audit team submitted "Data Request 32," in which the Audit team requested CDWR to provide facility connection requirements. On February 16, 2012, CDWR responded, and informed WECC that it understood itself to be exempt from FAC-001-0. CDWR explained that as a matter of policy, interconnections with other entities were not allowed. CDWR informed WECC that it did not have interconnections with other entities. The Audit team reviewed CDWR's Data Request Response, and determined that irrespective of CDWR's policy barring interconnection, CDWR must document and maintain interconnection requirements pursuant to R1 and R2. The Audit team also determined that CDWR's failure to provide documentation of connection requirements in response to Data Request 32 constituted an issue of FAC-001-0 R3. WECC determined that pursuant to FAC-001-0 R1, CDWR failed to document facility connection requirements in its capacity as a registered Transmission Owner. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Lastly, WECC determined that CDWR failed to make documentation available to WECC, the RRO within five days of its request for documentation of facility connection requirements per R3. WECC determined that CDWR documented and maintained Facility Connection Requirements as of July 16, 2012.	WECC 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 CDWR does not allow interconnection to its facilities, and has not had any interconnections. Absent interconnections, the risk posed by the failure to have facility connection requirements in compliance with FAC-001 R1, R2 and R3 is lessened.	CDWR submitted a Mitigation Plan CDWR documented and maintained facility connection requirements per FAC-001-1 R1 and R2 as of July 16, 2012.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	California Department of Water Resources (CDWR)	NCR05047	WECC2012009800	FAC-001-0	R2	During the course of an onsite Audit of CDWR compliance conducted between February 14, 2012, and February 24, 2012, the WECC Audit team determined that CDWR, as a Transmission Owner, was in noncompliance with FAC-001-0 R1, R2 and R3. Specifically, the Audit team determined that CDWR failed to document, maintain, and publish facility connection requirements per FAC-001-0 R1. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Further, the Audit Team determined that CDWR failed to make documentation available to WECC, the Regional Reliability Organization (RRO), within five days of its request for documentation of facility connection requirements per FAC-001-0 R3. On February 15, 2012, the Audit team submitted "Data Request 32," in which the Audit team requested CDWR to provide facility connection requirements. On February 16, 2012, CDWR responded, and informed WECC that it understood itself to be exempt from FAC-001-0. CDWR explained that as a matter of policy, interconnections with other entities were not allowed. CDWR informed WECC that it did not have interconnections with other entities. The Audit team reviewed CDWR's Data Request Response, and determined that irrespective of CDWR's policy barring interconnection, CDWR must document and maintain interconnection requirements pursuant to R1 and R2. The Audit team also determined that CDWR's failure to provide documentation of connection requirements in response to Data Request 32 constituted an issue of FAC-001-0 R3. WECC determined that pursuant to FAC-001-0 R1, CDWR failed to document facility connection requirements in its capacity as a registered Transmission Owner. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Lastly, WECC determined that CDWR failed to make documentation available to WECC, the RRO within five days of its request for documentation of facility connection requirements per R3. WECC determined that CDWR documented and maintained Facility Connection Requirements as of July 16, 2012.	WECC 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 CDWR does not allow interconnection to its facilities, and has not had any interconnections. Absent interconnections, the risk posed by the failure to have facility connection requirements in compliance with FAC-001 R1, R2 and R3 is lessened.	CDWR submitted a Mitigation Plan CDWR documented and maintained facility connection requirements per FAC-001-1 R1 and R2 as of July 16, 2012.
Western Electricity Coordinating Council (WECC)	California Department of Water Resources (CDWR)	NCR05047	WECC2012009801	FAC-001-0	R3	During the course of an onsite Audit of CDWR compliance conducted between February 14, 2012 and February 24, 2012, the WECC Audit team determined that CDWR, as a Transmission Owner, was in noncompliance with FAC-001-0 R1, R2 and R3. Specifically, the Audit team determined that CDWR failed to document, maintain, and publish facility connection requirements per FAC-001-0 R1. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Further, the Audit Team determined that CDWR failed to make documentation available to WECC, the Regional Reliability Organization (RRO), within five days of its request for documentation of facility connection requirements per FAC-001-0 R3. On February 15, 2012, the Audit team submitted "Data Request 32," in which the Audit team requested CDWR to provide facility connection requirements. On February 16, 2012, CDWR responded, and informed WECC that it understood itself to be exempt from FAC-001-0. CDWR explained that as a matter of policy, interconnections with other entities were not allowed. CDWR informed WECC that it did not have interconnections with other entities. The Audit team reviewed CDWR's Data Request Response, and determined that irrespective of CDWR's policy barring interconnection, CDWR must document and maintain interconnection requirements pursuant to R1 and R2. The Audit team also determined that CDWR's failure to provide documentation of connection requirements in response to Data Request 32 constituted an issue of FAC-001-0 R3. WECC determined that pursuant to FAC-001-0 R1, CDWR failed to document facility connection requirements in its capacity as a registered Transmission Owner. As a result, CDWR failed to specifically address the requirements specified in FAC-001 R2 in its facility connections. Lastly, WECC determined that CDWR failed to make documentation available to WECC, the RRO within five days of its request for documentation of facility connection requirements per R3. WECC determined that CDWR documented and maintained Facility Connection Requirements as of July 16, 2012.	WECC 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 CDWR does not allow interconnection to its facilities, and it has not had any interconnections. Absent interconnections, the risk posed by the failure to have facility connection requirements in compliance with FAC-001 R1, R2 and R3 is lessened.	CDWR submitted a Mitigation Plan CDWR documented and maintained facility connection requirements per FAC-001-1 R1 and R2 as of July 16, 2012.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Bonneville Power Administration (BPA)	NCR05032	WECC2012010063	FAC-501-WECC-	R3	On March 13, 2012, BPA, as a Transmission Owner, submitted a Self-Report citing possible noncompliance with FAC-501-WECC-1 R3. Specifically, BPA reported that it failed to follow its Transmission Maintenance and Inspection Plan (TMIP) in that it did not complete "Steel Tower Climb Inspections" at critical crossings every five years per its TMIP. WECC reviewed BPA's Self-Report. WECC determined that in addition to annual ground and aerial inspections, BPA's TMIP requires "Steel Tower Climb Inspections" at critical crossings every five years. WECC determined that although BPA completed annual ground and aerial inspections, BPA failed to perform Steel Tower Climb Inspections every five years for three lines on WECC transfer paths with 12 critical crossings.	WECC 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 although BPA did not complete "Steel Tower Climb Inspections" at critical crossings, on a five year interval, BPA did complete annual ground and aerial inspections for critical crossings and transmission lines.	In its Mitigation Plan, BPA stated that it completed all Steel Tower Climb Inspections and updated its work tracking system.
Western Electricity Coordinating Council (WECC)	Public Utility District No. 1 of Chelan County (CHPD)	NCR05338	WECC2012010849	INT-009-1	R1	On August 6, 2012, CHPD, as a Balancing Authority, submitted a Self-Report citing possible noncompliance with INT-009-1 R1. Specifically, CHPD reported it failed to implement a Confirmed Interchange as received from the Interchange Authority on 17 occasions between June 2, 2012, and July 16, 2012. WECC reviewed CHPD's Self-Report and contacted CHPD to request additional information. WECC determined that CHPD failed to implement 17 Confirmed Interchanges at the specified point in time on June 2, 2012, and July 16, 2012. WECC determined that 15 of the Confirmed Interchanges were not implemented as received, but were implemented within the hour. WECC also determined that the remaining two Confirmed Interchanges were not implemented as received, but were implemented at the end of the hour. Further, during discussions with WECC CHPD disclosed additional instances of possible noncompliance. Specifically, CHPD reported that on August 25, 2012, CHPD was required to implement a Confirmed Interchange at 6:00 a.m. CHPD disclosed that due to a shift change and operator error, the Confirmed interchange was implemented at 6:12 a.m. WECC therefore, found CHPD failed to implement a total of 18 Confirmed Interchanges.	WECC 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 in total CHPD implements more than 8,000 interchanges every year. Given the large number of Confirmed Interchanges implemented, the instant issue represents less than 1 percent of the total Confirmed Interchanges implemented by CHPD. Importantly, although CHPD did not implement the Confirmed Interchanges at the time prescribed by the Interchange Authority, CHPD quickly detected and implemented the Confirmed Interchanges thereby reducing the possibility of system imbalances or voltage overloads. CHPD quickly detected and mitigated possible noncompliance by implementing sixteen Confirmed Interchanges within the hour, and implementing two of the Confirmed Interchanges at the hour.	CHPD enhanced System Operator awareness on NERC requirements, CHPD responsibilities and the processes for implementing Interchange per the requirements of INT-009. System Operators each received a memorandum and packet of information for their review on July 30, 2012. The information included a flowchart showing the Interchange approval and implementation process, and their integral role in the process, as well as NERC standards INT-009 and INT-006, and two internal documents: System Operating Instruction No. 37 – Confirmation of NSI and NAI, and System Operating Guideline No. 45 – Corrective Actions for Slice Hourly Interchange Schedules. CHPD enhanced its alarming. CHPD added a new alarm code on July 25th, which triggers an alarm each time a new schedule has been received in WIT. The alarm sounds every 60 seconds until the schedule is forwarded. To mitigate the incident of noncompliance that occurred on August 25, 2012, CHPD disciplined the responsible transmission operator.
Western Electricity Coordinating Council (WECC)	Black Hills/Colorado Electric Utility Company, LP (BHCE)	NCR00089	WECC2012010604	PRC-005-1a	R2	On June 29, 2012, BHCE, as a Transmission Owner and Distribution Provider, self-reported noncompliance with PRC-005-1a R2. According to BHCE's Self-Report, BHCE failed to test and maintain one relay within its defined interval for a period of approximately 60 days. BHCE's CO2055 relay located at its WN Clark #2 Unit should have been maintained and tested by February 13, 2012, but was not tested until April 6, 2012.	WECC 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 entity tested shortly following its scheduled five-year interval and the relay had a functioning backup in place that had been maintained and tested within its defined interval.	To mitigate this violation BHCE maintained and tested the relay involved.
Western Electricity Coordinating Council (WECC)	Black Hills Colorado IPP, LLC (BHCI)	NCR11186	WECC2012010760	VAR-002-1.1b	R1	On July 20, 2012, BHCI, as a Generator Operator, self-certified potential noncompliance with VAR-002-1.1b R1. In addition, on July 3, 2012, BHCI submitted a Self-Report to WECC identifying potential noncompliance with VAR-002-1.1b. R1.3 because, from April 21, 2012 to April 23, 2012, it operated its PAGS Unit 43 not in Automatic Voltage Control (AVR) mode without notifying its Transmission Operator (TOP).	WECC 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 generator involved is a 29.5 MVA generator. In addition, BHCI has two other generating units at the facility rated a 71.2 MVA that were operating in AVR mode and capable to respond to voltage deviations.	BHCI operated is PAGS Unit 43 in AVR mode on April 23, 2012.
Western Electricity Coordinating Council (WECC)	Black Hills Colorado IPP, LLC (BHCI)	NCR11186	WECC2012010761	VAR-002-1.1b	R3	On July 20, 2012, BHCI, as a Generator Owner, self-certified potential noncompliance with VAR-002-1.1b R3. In addition, on July 3, 2012, BHCI submitted a Self-Report to WECC identifying potential noncompliance with VAR-002-1.1b. R3.4 because on April 23, 2012, it changed the status of its PAGS Unit 43 from manual mode to Automatic Voltage Control (AVR) mode without notifying its Transmission Operator (TOP) within 30 minutes.	WECC 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 although BHCI failed to notify its TOP of a status change of a reactive resource related to an AVR on a single generator, the status change resulted when BHCI switched the AVR to the AGC mode, as required by its TOP. Specifically, the TOP expected BHCI to operate this generator unit in AGC mode and was unaware that the generator was ever operating in manual mode. Accordingly, the TOP would have been operating the transmission line believing the generator involved was in AGC mode, which it was.	On April 27, 2012, BHCI notified its TOP that it was operating in AGC mode.

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	FRCC2011008471	CIP-006-1	R1; R1.1	FRCC_URE1 self-reported an issue with CIP-006-1 R1. Specifically, during an internal inspection of the Physical Security Perimeters (PSPs) at the primary energy control center (ECC) and a generation site, it was discovered that there was a gap in the existing six-wall border for two PSPs. One of the gaps was at the primary ECC and the other was at a generation site. Specifically, the gap at the generating plant was at a height of 12 feet and the opening was two feet tall and 8 feet wide. This gap was obstructed by insulation and other construction material. The gap at the ECC was at height of 15 feet and the opening was two feet tall and 10 feet wide, but was behind the reception area in the visitor's lobby of the ECC. The visitor's lobby is staffed by a receptionist during the normal working hours and the entrance door is locked outside of normal working hours. The front entrance is also monitored with a video camera monitoring device.	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 both of the facilities are restricted access. Although the PSP did not have a completely enclosed six-wall border, the openings were not visible or identifiable. There was no easy access to the openings and crawl space was limited by sufficient obstructions. Both of the facilities maintained proper monitoring and security controls for all outside access to the facility and only trusted and verified visitors are allowed on the premises.	To mitigate this issue, FRCC_URE1 immediately restricted access to the subject PSP by implementing a new temporary access procedure that included camera monitoring and posting of guards. FRCC_URE1 then extended the primary ECC PSP and added plywood restrictions at the generating plant.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008473	CIP-007-2a	R6	FRCC_URE1 self-reported an issue with CIP-007-2a R6. Specifically, a distributed control system (DCS) human machine interface (HMI) device within FRCC_URE1's generation site was being monitored by the security event monitoring system, but due to a communications failure, twenty-four hour a day, seven day a week (24/7) monitoring was lost. This condition existed for a period of approximately 45 days. The communication error was caused by an error in the internal clock of the device that expired the security event monitoring system account prematurely. For the duration of this issue, alarming was only available for communication failure and intrusion detection system alerts. The device at issue is a computer workstation used for chemistry control and monitoring of the water pH level in the boiler. The device is mostly active during start-up and otherwise is used mostly for periodic monitoring.	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 device was within a secured Physical Security Perimeter (PSP) and was not accessible remotely from outside the Electronic Security Perimeter (ESP). Even though cybersecurity event logs were not stored on the central log monitoring systems, additional logs were available on the local device to limit or analyze any additional risk that may have resulted from unauthorized access. FRCC_URE1 also maintained a network intrusion detection system to monitor the complete network and any unauthorized access. No unauthorized access was detected for the duration of the issue. Although FRCC_URE1 has one prior violation and one prior remediated issue with this Standard, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The prior violation for this requirement resulted from hardware failure of the log collector device and was promptly corrected by FRCC_URE1 after replacing the faulty device. The prior remediated issue was the result of late-filed Technical Feasibility Exceptions by FRCC_URE1, and is therefore not related to the instant issue.	To mitigate this issue, FRCC_URE1 re-established communication, set up a centralized time server and created a process for network devices which point to that machine to capture time. FRCC_URE1 also implemented automated rules to send an alert if a device that is being monitored by the access monitoring system does not communicate with the access monitoring system.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008536	CIP-007-1	R5; R5.1	FRCC_URE1 self-reported an issue with CIP-007-1 R5. Specifically, for five of its Cyber Assets, FRCC_URE1 did not ensure that individual and shared system accounts and authorized access permissions were consistent with the concept of “need to know” with respect to work functions performed, as required by R5.1. FRCC_URE1 also did not ensure that user accounts for these five systems were implemented as approved by the designated personnel, as documented in CIP-003-3 R5. These systems had individual and shared accounts but were pre-set to log in using a pre-configured account, allowing shared access to all users who had physical access to the system, instead of individual user access as required by the "need-to-know" concept.	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 devices were within a secured Physical Security Perimeter (PSP) and were not accessible remotely from outside the Electronic Security Perimeter (ESP). All five systems at issue had user accounts and associated passwords configured as required by the CIP Standards, but allowing pre-configured auto log-in could have allowed an unauthorized person to use unassigned privileges. However, the risk in this case was mitigated by the fact that only the five authorized personnel (with access to the subject shared account) had access to the PSP where the systems were located. Although FRCC_URE1 has three prior violations and one prior remediated issue with this Standard, the instant issue nonetheless does not represent a failure to mitigate a prior violation. One of FRCC_URE1's prior CIP-007 R5 violations and the prior issue involved FRCC_URE1's failure to file timely Technical Feasibility Exceptions, and are therefore unrelated to the instant issue. FRCC_URE1's second prior violation involved FRCC_URE1's failure to change default settings on access control and monitoring equipment. FRCC_URE1's third prior violation resulted from lack of documentation of shared accounts for certain Cyber Assets, but FRCC distinguishes this from the instant issue, which resulted from erroneous implementation and failed controls unrelated to the previous violation.	To mitigate this issue, FRCC_URE1 created a shared account for two of the systems that only allows personnel with account credentials to access the process network. On the other three systems, FRCC_URE1 shut down the automated default log-in and required access to be granted as needed to perform job duties.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008522	CIP-005-1	R3	FRCC_URE1 self-reported an issue with CIP-005-1 R3. Specifically, FRCC_URE1 failed to implement security monitoring processes to detect and alert for all actual unauthorized access into the Electronic Security Perimeters (ESPs) at one of its generation Critical Assets. FRCC_URE1 configured two access point devices to log traffic, including drops and denies, but failed to configure the access points to log all accepts. As a result, the logs were insufficient to demonstrate all actual unauthorized access at the two access points.	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 access points were correctly configured for logging and alerting all denies and drops, limiting the risk of unauthorized access. Although the access points were not configured to log successful log-ins, strong two-factor authentication was configured for all remote interactive access. Further, FRCC_URE1 utilized intrusion detection systems on all its perimeter devices and inside network traffic, limiting any external exploit.	To mitigate this issue, FRCC_URE1 corrected its access point entries to capture logs of all incoming requests. Previously these devices were configured to log failed and unsuccessful requests but not the successful requests. Further, FRCC_URE1 updated its policy and procedure for any new device to require logging of all traffic including accepts, drops, and denies.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100376	CIP-004-1	R2	During a Spot Check, MRO discovered that MRO_URE1 failed to review its cybersecurity training program annually. Specifically, MRO_URE1 failed to review training program material used to train third-party contractors and vendors that had access to its energy management system. MRO_URE1 relied on its vendors and contractors to train their own employees as required per a written agreement between the parties. However, MRO_URE1 did not review the training material provided to those vendors and contractor employees.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all of MRO_URE1's employees and contractor's received cybersecurity training within 90 days of being granted access. Additionally, although MRO_URE1 failed to review the training provided by its vendors and contractors annually, MRO_URE1 had a written agreement with its vendors and contractors which required them to provide training, and MRO_URE1 determined that the training program provided by the vendors and contractors met the requirements set forth in CIP-004-1 R2.	MRO_URE1 now collects annual training content from the vendors and contractors and reviews it annually, to ensure alignment with the required components and corporate policies. MRO verified that MRO_URE1 completed its mitigating activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100373	CIP-007-1	R5; R5.1.2	MRO_URE2 self-reported noncompliance with CIP-007-1 R5 because it failed to establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days for some Critical Cyber Assets. Specifically, access activity event logs were not kept on Front End Processing (FEP) equipment used in controlling bulk power system (BPS) remote terminal units. Logging was not possible because: (1) FEP configuration for log events did not include user access activity events and was not configured with clock source or timestamp logs; (2) hardware was unable to support the operating system version that performs logging of user access activity; and (3) the electric SCADA application was unable to support current operating system features to perform logging of user access activity through remote authentication via the access control system server. The issue was resolved with a system upgrade.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because less than 6% of MRO_URE2's FEP devices were incapable of generating logs, and these FEPs do not control major BPS equipment and are mainly used for distribution breakers, voltage regulators and capacitors. In addition, all communications from the FEPs to the field is done through serial communications. Also, the devices without configured logging were within an Electronic Security Perimeter and a Physical Security Perimeter with documented firewall rules and implemented network traffic monitoring systems.	MRO_URE2 performed the following mitigating actions: (1) researched operating system versions available on existing hardware to try to find one that will run with the current memory and provide features that perform logging of user access activity; (2) configured and tested remote authentication via the access control server to try to capture user access activity events in the log without breaking the SCADA application functionality; and (3) performed a full system upgrade and removed the equipment from the NERC CIP inventory. The upgrade included a complete hardware and software replacement and the configuration of necessary logging controls. MRO verified that MRO_URE2 completed its mitigating activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100382	CIP-004-1	R2	During a Spot Check, MRO discovered that MRO_URE2 failed to review its cybersecurity training program annually. Specifically, MRO_URE2 failed to review training program material used to train third-party contractors and vendors that had access to its energy management system. MRO_URE2 relied on its vendors and contractors to provide training to their employees as required per a written agreement between the parties. However, MRO_URE2 did not review the training material provided to those vendors and contractor employees.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all of MRO_URE2's employees and contractor's received cybersecurity training within 90 days of being granted access. Additionally, although MRO_URE2 failed to review the training provided by its vendors and contractors annually, MRO_URE2 had a written agreement with its vendors and contractors which required them to provide training, and MRO determined that the training program provided by the vendors and contractors complied with the requirements set forth in CIP-004-1 R2.	MRO_URE2 now collects annual training content from the vendors and contractors and reviews it annually, to ensure alignment with the required components and corporate policies. MRO verified that MRO_URE2 completed its mitigating activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3)	NCRXXXXX	MRO201100313	CIP-006-1	R6; R6.1	During a regularly scheduled Compliance Audit, MRO discovered that MRO_URE3 failed to demonstrate that all physical security mechanisms had been tested on a cycle no longer than three years. Although MRO_URE3 conducted comprehensive testing of access and monitoring controls two times in 2010, it did not conduct any testing prior to those dates. Two of the card readers were installed or reconfigured more than three years prior to the 2010 testing. MRO_URE3 failed to test 46% of its access points within the three-year cycle.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The access points that were not tested until the first instance in 2010 were access points to the dispatch room, which is staffed with personnel 24 hours per day, seven days per week. Additionally, MRO_URE3's physical access control system logs demonstrated that the access points were working throughout the duration of the compliance issue. Finally, MRO_URE3 tested all of its access points at least annually between 2010 and 2012.	MRO_URE3 completed testing and maintenance of all physical security mechanisms. MRO verified that MRO_URE3 completed its mitigating activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012009157	CIP-007-1	R4.1	During an on-site Compliance Audit, NPCC discovered that NPCC_URE1 had an issue with CIP-007-1 R4.1. During the course of fieldwork and in reviewing various NPCC_URE1 network diagrams, NPCC discovered that eight devices in total residing at four different substations were contained within the Electronic Security Perimeter (ESP) and not equipped with anti-virus and malware prevention tools. The eight devices at issue do not run on an operating system which supports or allows the installation of anti-virus and malware prevention tools, but NPCC_URE1 neglected to file a Technical Feasibility Exception (TFE) request with NPCC.	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 NPCC_URE1's procedure limited employee electronic access. Additionally, NPCC_URE1 has, since June 30, 2009, had protections in place for assets inside the ESP, such as firewall protection, device authentication, and network security monitoring. This is an open-ended TFE because the hardened operating system in question does not support third-party software.	This issue was mitigated through the TFE process. NPCC_URE1 filed the Part A TFE with NPCC. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011007720	CIP-006-2	R6	NPCC_URE2 self-reported an issue with CIP-006-2 R6 for a period of approximately 14 months. During this period, NPCC_URE2's procedure incorrectly stated the requirement for logging physical entry into a Physical Security Perimeter (PSP) to be limited to the initial entry at the start of the work day. Once a NPCC_URE2 worker utilized his or her credentials to enter the PSP, the worker would then exit and re-enter the PSP as the work day progressed. For example, after an initial entry and logging, a worker would exit the PSP to retrieve tools and then re-enter the PSP to continue work, which he or she did without re-logging entry. This issue is limited to those persons who were granted authorized unescorted access to PSPs.	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 employees that were not re-logging entry into the PSP were all authorized for unescorted access.	NPCC_URE2 mitigated this issue by updating the governing operating procedure to include logging workers' entry and exit each time they enter the PSP and providing in-person training. The training consisted of a review of changes to the operating procedure and a review of the proper way to enter and exit the PSP.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011007721	CIP-006-2	R6	NPCC_URE2 self-reported an issue with CIP-006-2 R6 for a period of approximately 14 months. This issue relates to those persons (Visitors) not granted authorized unescorted access to Physical Security Perimeters (PSPs). During this period, NPCC_URE2's procedure incorrectly stated the requirement for logging physical entry into a PSP to be limited to the initial entry at the start of the work day, and final exit at the end of the work day. Once a Visitor was escorted into the PSP, the Visitor would then proceed to exit and re-enter the PSP as the work day progressed. For example, after an initial entry and logging, a Visitor would exit the PSP to retrieve tools and then re-enter the PSP to continue work, which he or she did without re-logging entry. At the conclusion of the work day, the Visitor would log the exit time.	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 locations in question were in field control houses that were being staffed by NPCC_URE2 employees with authorized unescorted access at the time, and the Visitors were continuously escorted while in the PSP.	NPCC_URE2 mitigated this issue by updating the governing operating procedure to include correctly logging Visitors' access to PSPs and completing in-person training with persons with unescorted physical access to the PSP. The training consisted of a review of changes to the operating procedure and a review of the proper way to enter and exit the PSP and escort visitors.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011007722	CIP-006-3c	R1.6	NPCC_URE2 self-reported an issue with CIP-006-3c R1.6. This issue relates to those persons (Visitors) not granted authorized unescorted access to Physical Security Perimeters (PSPs). On the effective compliance enforcement date of CIP-006-3c, NPCC_URE2 had procedures for escorting Visitors and logging Visitor entry and exit to and from PSPs. NPCC_URE2 interpreted the requirement of CIP-006-3 R1.6 to be consistent with the existing logging practice associated with CIP-006-3 R6. NPCC_URE2 incorrectly understood the requirement for logging physical entry into a Physical Security Perimeter (PSP) to be limited to the initial entry at the start of the work day and final exit at the end of the work day. Once a Visitor was escorted into the PSP, the Visitor would then proceed to exit and re-enter the PSP as the work day progressed. For example, a Visitor would exit the PSP to retrieve tools and then re-enter the PSP to continue work, which he or she did without re-logging entry. At the conclusion of the work day, the Visitor would log the exit time. The Visitors were continuously escorted while in the PSP.	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 locations in question were in field control houses that were being staffed by NPCC_URE2 employees with authorized unescorted access at the time, and the Visitors were continuously escorted while in the physical security perimeter.	NPCC_URE2 mitigated this issue by updating the governing operating procedure to include correctly logging Visitors' access to PSPs and completing in-person training with persons with unescorted physical access to the PSP. The training consisted of a review of changes to the operating procedure and a review of the proper way to log access to PSPs and to escort visitors.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011007723	CIP-006-2	R5	NPCC_URE2 self-reported an issue with CIP-006-2 R5 for a period of approximately sixteen months. NPCC_URE2 monitors physical access at access points to the Physical Security Perimeter (PSP) via a remote guard station, known as the monitoring station. When a door is opened without an electronic card being utilized to unlock the door, a "forced door open" (FDO) alarm is generated and observed at the monitoring station. The security officer is provided a standing desk procedure, which requires the officer to call the substation. If an authorized person answers the phone, the officer is to acknowledge and clear the alarm. If no one answers the officer is required to: (a) contact the designated on-call supervisor for a response, and (b) check the substation camera system to determine if the unauthorized access (break-in) can be confirmed. If an unauthorized access attempt is confirmed, the officer is required to contact local police and the on-call supervisor immediately. If unauthorized access cannot be confirmed through the camera system, the officer is to notify the on-call supervisor for a response. If an unauthorized access is confirmed by the supervisor, then the cyber incident response plan is activated. NPCC determined that NPCC_URE2's security officer did not follow the standing desk procedure for determining if an unauthorized access attempt had occurred. In lieu of following the standing desk procedure, the security officer, when receiving a FDO alarm, would properly acknowledge the alarm on the monitor and then determine if the person in the substation was a NPCC_URE2 employee by utilizing the camera system and waiting for the person to utilize the electronic key at another access point to the PSP.	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 security officer was following a process to conclude that an actual breach did not occur.	NPCC_URE2 mitigated this issue by: (1) updating its operating procedure, including the desk procedure at issue, to include responding to alarms; (2) ensuring that each security officer reviewed the desk procedure for responding to an intrusion alarm; and (3) reviewing the operating procedure with the security officers to reinforce the response requirements to an alarm, the process to enter and exit substations, and visitor logging.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011009011	CIP-008-2	R1.4	NPCC_URE2 self-reported an issue with CIP-008-2 R1.4. On April 1, 2010, Version 2 of NERC Standard CIP-008 became effective and changed the requirement for updating the Cyber Security Incident response plan from within 90 days to within 30 days of a change. NPCC_URE2 revised its Cyber Security Incident Response & Reporting Plan (Plan) but did not include the change in requirement from 90 to 30 days. NPCC_URE2 revised its Plan again the following year as part of the annual review and again did not identify this error. Later that year, UI identified the error in its Plan and corrected the error.	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 issue is a documentation error and administrative in nature.	NPCC_URE2 mitigated this issue by correcting and updating its Plan from 90 days to 30 days.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011009012	CIP-007-1	R5.3	NPCC_URE2 self-reported an issue with CIP-007-1 R5.3. NPCC_URE2's physical access control system utilizes four Cyber Assets that are required to comply with the password requirements of CIP-007-1 R5.3. First, NPCC_URE2 reported that 11 accounts on the operating system did not have passwords changed annually, as required by the Standard. These issues were discovered during a cyber vulnerability assessment. Second, NPCC_URE2 was notified by the vendor conducting the cyber vulnerability assessment that two passwords were not changed annually, and NPCC_URE2 then corrected those issues. Subsequently, NPCC_URE2 requested information from the vendor about any other passwords that were greater than 365 days old on this system and was informed that an additional nine passwords were not compliant and NPCC_URE2 corrected those. The passwords are associated with administrative and user accounts for the operating systems on these four Cyber Assets.	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 devices at issue are located within an access controlled room. Additionally, there is no remote access to the devices.	NPCC_URE2 mitigated this issue by disabling or changing the accounts identified in the Self-Report. NPCC_URE2 reviewed the final cyber vulnerability assessment report for similar account and password violations and found none. In addition, NPCC_URE2 issued a memo to the managers of Cyber Assets reinforcing the need to change passwords at least annually and to verify accounts annually at both the application and operating system level.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008240	CIP-006-1	R1.2	NPCC_URE3 self-reported an issue with CIP-006-1 R1.2. NPCC_URE3 discovered that two emergency exit-only doors on the Physical Security Perimeter (PSP) were not identified as physical access points. Additionally, the access control alarms for the two emergency exit-only doors were not configured in NPCC_URE3's physical access control intrusion detection system to alarm upon opening as a CIP alarm. Although the two emergency exit-only doors were configured to report any activity to the access control intrusion detection system alarm history log, this is not the required configuration. The required configuration is that opening the door (defined as a break in the door contacts in the door and frame) will trigger an alarm in the access control intrusion detection system for resolution and the unique determination of the emergency exit-only door usage by NPCC_URE3's centralized security operations center.	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 PSP is manned 24 hours a day, seven days a week by authorized personnel. Second, NPCC_URE3 conducts annual training and quarterly re-enforcement training for the recognition and reporting of suspicious activity for site personnel. Third, the site is regulated under the Maritime Transportation Security Act of 2002, which requires stringent physical security measures, including prohibiting an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued transportation worker identification credential and is authorized to be in the area. Lastly, the two emergency exit-only doors are not able to be opened from the outside without a special tool, which was not readily available.	NPCC_URE3 mitigated this issue by: (1) issuing a security awareness bulletin to the CIP area access managers and compliance managers on the proper use of physical access points and how to detect an issue with or misuse of a physical access point or physical security protection; (2) updating corporate security procedure on how to conduct a physical walk-down of a PSP and its physical access points before a site is declared compliant; (3) labeling and identifying in the physical security plan drawing the two emergency exit doors as access points, and approving the drawings and uploading them to the appropriate documentation office; (4) performing a door check and reviewing output of the door check with site personnel; (5) reconfiguring the two emergency exit only doors and verifying that opening of the door generates an alarm to the security operations center; (6) training corporate security personnel on the updated procedure; (7) updating yearly awareness training for corporate security personnel of their requirements for a site-walk down; and (8) extending the event analysis procedure to be completed at each of the regulated PSPs to include a review and physical walk-down of all the “six-wall” physical access points to ensure that each physical access point is identified on the physical security drawing, as well as within the access control intrusion detection system.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008241	CIP-006-1	R4	NPCC_URE3 self-reported an issue with CIP-006-1 R4. NPCC_URE3 discovered that two emergency exit-only doors on the Physical Security Perimeter (PSP) were not identified as physical access points. As a result of this, NPCC_URE3 did not implement and document the technical and procedural mechanisms for logging physical entry at these two access points for a period of approximately 21 months.	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 PSP is manned 24 hours a day, seven days a week by authorized personnel. Second, NPCC_URE3 conducts annual training and quarterly re-enforcement training for the recognition and reporting of suspicious activity for site personnel. Third, the site is regulated under the Maritime Transportation Security Act of 2002, which requires stringent physical security measures, including prohibiting an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued transportation worker identification credential and is authorized to be in the area. Lastly, the two emergency exit-only doors are not able to be opened from the outside without a special tool, which was not readily available.	NPCC_URE3 mitigated this issue by: (1) issuing a security awareness bulletin to the CIP area access managers and compliance managers on the proper use of physical access points and how to detect an issue with or misuse of a physical access point or physical security protection; (2) updating corporate security procedure on how to conduct a physical walk-down of a PSP and its physical access points before a site is declared compliant; (3) labeling and identifying in the physical security plan drawing the two emergency exit doors as access points, and approving the drawings and uploading them to the appropriate documentation office; (4) performing a door check and reviewing output of the door check with site personnel; (5) reconfiguring the two emergency exit only doors and verifying that opening of the door generates an alarm to the security operations center; (6) training corporate security personnel on the updated procedure; (7) updating yearly awareness training for corporate security personnel of their requirements for a site-walk down; and (8) extending the event analysis procedure to be completed at each of the regulated PSPs to include a review and physical walk-down of all the “six-wall” physical access points to ensure that each physical access point is identified on the physical security drawing, as well as within the access control intrusion detection system.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008242	CIP-006-1	R3	NPCC_URE3 self-reported an issue with CIP-006-1 R3. NPCC_URE3 discovered that two emergency exit-only doors on the Physical Security Perimeter (PSP) were not identified as physical access points. Additionally, the access control alarms for the two emergency exit-only doors were not configured in NPCC_URE3's physical access control intrusion detection system to alarm upon opening as a CIP alarm. Although the two emergency exit-only doors were configured to report any activity to the access control intrusion detection system alarm history log, this is not the required configuration. The required configuration is that opening the door (defined as a break in the door contacts in the door and frame) will trigger an alarm in the access control intrusion detection system for resolution and the unique determination of the emergency exit-only door usage by NPCC_URE3's centralized security operations center.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the PSP is manned 24 hours a day, seven days a week by authorized personnel. Second, NPCC_URE3 conducts annual training and quarterly re-enforcement training for the recognition and reporting of suspicious activity for site personnel. Third, the site is regulated under the Maritime Transportation Security Act of 2002, which requires stringent physical security measures, including prohibiting an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued transportation worker identification credential and is authorized to be in the area. Lastly, the two emergency exit-only doors are not able to be opened from the outside without a special tool, which was not readily available.	NPCC_URE3 mitigated this issue by: (1) issuing a security awareness bulletin to the CIP area access managers and compliance managers on the proper use of physical access points and how to detect an issue with or misuse of a physical access point or physical security protection; (2) updating corporate security procedure on how to conduct a physical walk-down of a PSP and its physical access points before a site is declared compliant; (3) labeling and identifying in the physical security plan drawing the two emergency exit doors as access points, and approving the drawings and uploading them to the appropriate documentation office; (4) performing a door check and reviewing output of the door check with site personnel; (5) reconfiguring the two emergency exit only doors and verifying that opening of the door generates an alarm to the security operations center; (6) training corporate security personnel on the updated procedure; (7) updating yearly awareness training for corporate security personnel of their requirements for a site-walk down; and (8) extending the event analysis procedure to be completed at each of the regulated PSPs to include a review and physical walk-down of all the “six-wall” physical access points to ensure that each physical access point is identified on the physical security drawing, as well as within the access control intrusion detection system.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008243	CIP-006-1	R2	NPCC_URE3 self-reported an issue with CIP-006-1 R2. NPCC_URE3 discovered that two emergency exit-only doors on the Physical Security Perimeter (PSP) were not identified as physical access points. As the result of this, NPCC_URE3 did not document and implement the technical and procedural controls to manage physical access at these two access points 24 hours a day, seven days a week.	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 PSP is manned 24 hours a day, seven days a week by authorized personnel. Second, NPCC_URE3 conducts annual training and quarterly re-enforcement training for the recognition and reporting of suspicious activity for site personnel. Third, the site is regulated under the Maritime Transportation Security Act of 2002, which requires stringent physical security measures, including prohibiting an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued transportation worker identification credential and is authorized to be in the area. Lastly, the two emergency exit-only doors are not able to be opened from the outside without a special tool, which was not readily available.	NPCC_URE3 mitigated this issue by: (1) issuing a security awareness bulletin to the CIP area access managers and compliance managers on the proper use of physical access points and how to detect an issue with or misuse of a physical access point or physical security protection; (2) updating corporate security procedure on how to conduct a physical walk-down of a PSP and its physical access points before a site is declared compliant; (3) labeling and identifying in the physical security plan drawing the two emergency exit doors as access points, and approving the drawings and uploading them to the appropriate documentation office; (4) performing a door check and reviewing output of the door check with site personnel; (5) reconfiguring the two emergency exit only doors and verifying that opening of the door generates an alarm to the security operations center; (6) training corporate security personnel on the updated procedure; (7) updating yearly awareness training for corporate security personnel of their requirements for a site-walk down; and (8) extending the event analysis procedure to be completed at each of the regulated PSPs to include a review and physical walk-down of all the “six-wall” physical access points to ensure that each physical access point is identified on the physical security drawing, as well as within the access control intrusion detection system.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012009964	CIP-007-3	R5.3	NPCC_URE4 self-reported an issue with CIP-007-3 R5.3. Specifically, 20 NPCC_URE4 Cyber Assets within the Electronic Security Perimeter (ESP) did not have technical controls for strict compliance with the password requirements of R5.3, and the Cyber Assets were not covered under an existing Technical Feasibility Exception (TFE). NPCC_URE4 failed to submit a TFE request for all 20 Cyber Assets.	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 of the compensatory procedures and technical controls that NPCC_URE4 implemented. Access to the devices at issue is monitored. Physical access is required to configure the devices, and physical access controls restrict unauthorized physical access. Additionally, NPCC_URE4's operating procedures require that passwords meet minimum length requirements and personnel are trained on the procedures. NPCC_URE4's minimum password strength exceeds requirements. NPCC_URE4's operating procedures require that passwords are changed at least annually and personnel are trained on the procedures. The operating procedures require that passwords contain the required combination of characters. Complex password policy has been enabled on the devices at issue. Also, these devices have been configured to require a minimum password length of eight characters. The resulting passwords exceed the password complexity required by CIP-007-3 R5.3. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE4 filed the Part A TFE. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2012010462	CIP-007-1	R3	NPCC_URE5 self-reported an issue with CIP-007-1 R3. Specifically, 14 NPCC_URE5 devices were not able to be patched because security patches are no longer supplied by the application vendors. NPCC_URE5 failed to submit Technical Feasibility Exception (TFE) requests for all 14 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 of the compensatory procedures and technical controls that NPCC_URE5 implemented. The devices at issue are protected in that all reside within Physical Security Perimeters (PSPs) and Electronic Security Perimeter (ESP). The incident response plan will notify support personnel to take action in the event a device is compromised; the facility IT contact will interface with the Corporate Cyber Incident Response Team to provide assistance with communication and remediation. Lastly, network isolation prevents exposure of these devices to un-trusted networks, including the internet and business network. These are open-ended TFEs.	This issue was mitigated through the TFE process. NPCC_URE5 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFEs approval.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2012010463	CIP-007-1	R4.1	NPCC_URE5 self-reported an issue with CIP-007-1 R4. Specifically, the operating systems on 54 devices did not have anti-virus and anti-malware tools installed and therefore were not patched on a regular basis. NPCC_URE5 failed to submit Technical Feasibility Exception (TFE) requests for all 54 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 of the compensatory procedures and technical controls that NPCC_URE5 implemented. The devices at issue are protected by the Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP), which are controlled and monitored. Network isolation also prevents exposure of the devices to un-trusted networks, including the internet and business networks. Additionally, the incident response plan will notify support personnel to take action in the event a device is compromised; the facility IT contact will interface with the Corporate Cyber Incident Response Team to provide assistance with communication and remediation. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE5 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFEs approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2012010464	CIP-007-1	R5.3	NPCC_URE5 self-reported an issue with CIP-007-1 R5. Specifically, the operating systems on 54 devices do not have technical controls for password length, character complexity, or password change frequency, as required by CIP-007-1 R5.3. NPCC_URE5 failed to submit Technical Feasibility Exception (TFE) requests for all 54 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 of the compensatory procedures and technical controls that NPCC_URE5 implemented. First, the devices at issue are protected by the Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP). Additionally, personnel risk assessments and training ensure that only vetted personnel have access to these devices. Lastly, proprietary machine language for instructions inhibits plug-in and control by a potential hacker. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE5 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFEs approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010500	CIP-007-1	R3	NPCC_URE6 self-reported that one device could not being patched, resulting in an issue with CIP-007-1 R3. NPCC_URE6 failed to submit a Technical Feasibility Exception (TFE) request for this device.	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 of the compensatory procedures and technical controls that NPCC_URE6 implemented. The device at issue is protected by the fact that it resides within a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The incident response plan will notify support personnel to take action in the event the device is compromised; the Facility IT contact will interface with the Corporate Cyber Incident response team providing assistance with communication and remediation. Network isolation prevents exposure of device to un-trusted networks, including the Internet and business network. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE6 filed the Part A TFE. NPCC accepted the Part A TFE. NPCC completed and accepted the Part B TFE approval.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010501	CIP-007-1	R4.1	NPCC_URE6 self-reported an issue with CIP-007-1 R4. Specifically, the operating systems on five devices did not have anti-virus and anti-malware tools installed. NPCC_URE6 failed to submit Technical Feasibility Exception (TFE) requests for all five 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 of the compensatory procedures and technical controls that NPCC_URE6 implemented. The devices at issue are protected by the fact that they reside within a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The incident response plan will notify support personnel to take action in the event a device is compromised; the Facility IT contact will interface with the Corporate Cyber Incident response team providing assistance with communication and remediation. Network isolation prevents exposure of device to un-trusted networks, including the Internet and business network. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE6 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFE approvals.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010502	CIP-007-1	R5.3	NPCC_URE6 self-reported an issue with CIP-007-1 R5.3. Specifically, one device did not have technical controls for password length, character complexity, or password change frequency. NPCC_URE6 failed to submit Technical Feasibility Exception (TFE) requests for this device.	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 of the compensatory procedures and technical controls that NPCC_URE6 implemented. The device at issue is protected by the fact that it resides within a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The incident response plan will notify support personnel to take action in the event the device is compromised; the Facility IT contact will interface with the Corporate Cyber Incident response team providing assistance with communication and remediation. Network isolation prevents exposure of device to un-trusted networks, including the Internet and business network. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE6 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFE approvals.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010503	CIP-007-1	R6	NPCC_URE6 self-reported an issue with CIP-007-1 R6. Specifically, two devices were not capable of generating internal logs of system events including security and authentication-related incidents. NPCC_URE6 failed to submit Technical Feasibility Exception (TFE) requests for these 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 of the compensatory procedures and technical controls that NPCC_URE6 implemented. The devices at issue are protected by the fact that they reside within a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The incident response plan will notify support personnel to take action in the event a device is compromised; the Facility IT contact will interface with the Corporate Cyber Incident response team providing assistance with communication and remediation. Network isolation prevents exposure of device to un-trusted networks, including the Internet and business network. This is an open-ended TFE.	This issue was mitigated through the TFE process. NPCC_URE6 filed the Part A TFEs. NPCC accepted the Part A TFEs. NPCC completed and accepted the Part B TFE approvals.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010441	CIP-006-3a	R1	During a compliance audit, Reliability*First* discovered that RFC_URE1 had an issue with CIP-006-3c R1.6. RFC_URE1 failed to maintain completed visitor logs in certain instances. ReliabilityFirst discovered deficiencies on four dates where visitor logs were missing exit or log out information.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. RFC_URE1 has in place an internal auditing system of its visitor logs where, every few days, its security personnel ensure that the logs contain the correct information. RFC_URE1, therefore, noticed the discrepancies in the logs and corrected them within a few days of the discrepancies occurring.	RFC_URE1 performed the following mitigating activities: 1) reinforced the visitor procedure requirements with the appropriate individuals, including executives; 2) held a meeting with operations managers to discuss NERC CIP issues including the requirement for visitor procedures; and 3) reinforced the visitor procedure through posted signage, training, and ongoing awareness measures.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010442	CIP-007-3	R9	During a compliance audit, Reliability*First* discovered that RFC_URE1 had an issue with CIP-007-1 R9. For one of its CIP-007 documents, RFC_URE1 performed an annual review in 2010 and 2011, but failed to document all changes resulting from modifications to the systems or controls within thirty calendar days of completing the changes. Instead, RFC_URE1 gradually documented the changes in a manner which resulted in several versions where it was unclear which date applied to which change. In two instances, RFC_URE1 documented changes four months and two months after modifications, past the 30 days required by the Standard.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that RFC_URE1 documented the changes resulting from modifications to the systems or controls within four months for 2010 and within two months for 2011, although not within the required 30 days. Although RFC_URE1 could not provide documentation as evidence of completed the updates, RFC_URE1 asserted that it had actually completed the updates within 30 calendar days.	RFC_URE1 documented the changes resulting from modifications to the systems or controls. In addition, RFC_URE1 now utilizes software to more effectively document the dates it makes modifications.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010444	CIP-005-1	R4	During a compliance audit, Reliability*First* discovered that RFC_URE1 had an issue with CIP-005-1 R4. A third-party vendor performs RFC_URE1 cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter (ESP). RFC_URE1 third-party vendor deleted the detailed evidence related to the cyber vulnerability assessment. As a result, RFC_URE1 provided a summary report from the third-party vendor that it: (a) performed a review to verify that only ports and services required for operations at electronic access points to the ESP were enabled (R4.2); (b) included the discovery of all access points to the ESP (R4.3); and (c) performed a review of controls for default accounts, passwords, and network management community strings (R4.4). RFC_URE1, however, was unable to provide detailed evidence to support the summary report and that it had fulfilled all the subrequirements of R4.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. RFC_URE1 performed the required actions in its cyber vulnerability assessment and provided a summary of the cyber vulnerability assessment. RFC_URE1's evidence was simply inadequate to demonstrate the extent of RFC_URE1's cyber vulnerability assessment.	RFC_URE1 revised its cyber vulnerability assessment procedure with the vendor to ensure detailed requirements for performing the assessment and to ensure production of evidence and retention of the evidence to support the evaluation of the state of the controls measured against the Reliability Standards. In addition, the procedure requires the final evaluation of all requirements to be substationed with detailed evidence to support all conclusions.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) Southern Company Services, Inc. - Trans (SCS-Trans)	NCRXXXXX	SERC200900395	CIP-003-1	R1.2	The SERC Spot Check team reported an issue with CIP-003-1 R1.2, stating that SERC_URE1 failed to provide evidence that its cyber security policy (CSP) was readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets (CCAs). During the CIP Spot Check, SERC_URE1 indicated that personnel were only able to access the portions of the CSP that were deemed applicable to their job responsibilities and not the entire CSP. SERC staff requested and reviewed additional information in order to complete its assessment. SERC staff learned that the CSP consisted of multiple variations that were available to provide the level of detail pertinent to the roles and responsibilities of the person with access to or responsibility for CCAs. These various abridged role-based CSPs also contained operational data that assisted the employee in performance of their specific duties. SERC_URE1 made the CSP readily available by placing the CSP required by the employee's role on the SERC_URE1 intranet. SERC_URE1 also covered the CSP in its annual cyber security training pursuant to CIP-004 R2. In the training, SERC_URE1 informed each user where to find the training on the intranet, as well as contact information if the user needed or wished to receive a copy of the CSP. If the trainee did not have access to the intranet and the online training, the trainer would cover the CSP at the time of the training and would also provide the trainee with contact information for a copy of the CSP and with any questions after the training concluded. The trainer was typically a senior employee or supervisor, and trainers typically advised trainees to see their manager or any employee with intranet access for a copy of the CSP. Only 3.5% of personnel with CCA access did not have log-in capabilities to the intranet at the time of the Spot Check.	SERC staff 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: 1. SERC_URE1 provided applicable portions of the CSP to personnel based on the roles and responsibilities they were performing; and 2. Only 3.5% of personnel with access to CCAs did not have intranet access and needed to depend on their manager or other users to obtain a hard copy of the CSP. These individuals were told during cyber security training who they could contact for a copy of the full CSP.	SERC staff verified that SERC_URE1 completed the following actions: 1. Revised the CSP to more clearly address CIP-002 through CIP-009, and to incorporate and supersede all associated policies and procedures; 2. Electronically posted the revised policy both internally and on SERC_URE1's website so that it may be readily accessible by all personnel with electronic access; 3. Physically placed the revised policy at each of SERC_URE1's Physical Security Perimeters so that it is readily accessible by all personnel with physical access; and 4. Notified all personnel with access to CCAs of the revised CSP and the various places it will be readily available.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000246	CIP-003-1	R4	During the course of a Multi-Region Spot Check, SPP RE found SPP RE_URE1 to be in noncompliance with CIP-003-1 R4 for failing to identify, classify, and protect information associated with Critical Cyber Assets (CCAs). Specifically, SPP RE_URE1 failed to label certain documents as prescribed in its energy information security classification policy. Subsequent to the CIP Spot Check, SPP RE_URE1's parent company conducted an overarching review of documents affected by the energy information security classification policy as part of the measures used to mitigate this particular remediated issue. SPP RE_URE1's parent company found 18 additional documents that were not labeled appropriately, four of which belonged to SPP RE_URE1.	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 documents that were not labeled as prescribed by SPP RE_URE1's energy information security classification policy were in electronic form at the time the issue occurred. SPP RE_URE1 has a document software package for document security which limits electronic access to authorized users, thus protecting SPP RE_URE1's information associated with its CCAs. The documents which were not marked confidential in accordance with the SPP RE_URE1 energy information security classifications policy were restricted access documents within the SPP RE_URE1 document security system. Only a limited number of authorized users were able to access the documents.	SPP RE_URE1 performed the following actions to mitigate the issue: 1) conducted a comprehensive review to ensure compliance with all requirements under CIP-003-1; and 2) marked all relative documents in accordance with its energy information security classification policy.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012010061	CIP-004-3	R3	WECC_URE1 submitted a Self-Report addressing an issue with this Standard. According to the Self-Report, during a routine review of personnel risk assessment (PRA) tickets, the WECC_URE1 Human Resource Department identified a PRA that was not renewed seven years after the initial assessment. WECC_URE1 stated the overdue PRA is for a control room operator with both physical and cyber access to the supervisory control and data acquisition (SCADA) system inside the control rooms Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). WECC_URE1 stated further that the operator's completion of the most current PRA was five weeks beyond the CIP-004 R3.2 allowable timeframe. According to WECC_URE1, upon identification of the overdue PRA, Human Resources immediately informed Physical Security who took action to initiate the overdue PRA. The PRA was completed within 24 hours of its discovering its expiration. WECC concluded that WECC_URE1 had an issue of CIP-004-3 R3 for failing to renew the control room operator's PRA within seven years as required by R3.2. WECC determined that WECC_URE1 had an issue of CIP-004-3 R3.2 for failing to timely renew the PRA for one employee.	WECC 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 although WECC_URE1 failed to timely renew a PRA, the operator in scope had a previous PRA, had completed current CIP training, and was a long time employee who had authorized access to the control room to perform his daily duties. Also, the SCADA system resides within the control room's PSP and ESP with continuous video monitoring. Additionally, WECC_URE1 employs onsite security personnel at all access points and at all PSPs.	WECC_URE1 submitted a Mitigation Plan to address this issue. The Mitigation Plan required WECC_URE1 to: (1) redeploy the individual responsible for initiating the PRA process; (2) review the current CCA holders to verify that all PRAs are current; (3) begin duplicate monitoring of PRAs. This process included the creation of daily reports that lists the pending PRAs 90 days in advance and recently completed PRAs. Also, this process incorporates a review of PRA status during WECC_URE1's annual badge renewal cycle; and (4) Human Resources will independently monitor the completion of PRAs and escalate to management any PRA tickets that are not closed within the first month.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010524	CIP-004-3	R2	WECC_URE2 submitted a Self-Report citing noncompliance with CIP-004-3 R2. Specifically, WECC_URE2 reported that a contractor was granted cyber access to Critical Cyber Assets (CCAs) prior to completing cyber security training. WECC determined that on WECC_URE2 granted a contractor access to CCAs prior to his completion of cyber security training. WECC also determined that PGE detected and revoked the contractor's access rights within that same day.	WECC 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 risk posed by WECC_URE2 noncompliance is offset given the duration and scope, as well as by compensating measures in place during the issue period. The scope of the issue was limited to a single individual with cyber access to CCAs associated with the control center and backup control center for a period of a single day. Within hours of granting the contractor access, WECC_URE2 detected its error. WECC_URE2 revoked the contractor's access. During the period in which the contractor had access to CCAs, there were a number of compensating security measures in place that offset the risk of possible noncompliance with R2.1. The CCAs were protected by an electronic intrusion detection system. All access to CCAs was logged and monitored. Further, the CCAs were physically secured within a Physical Security Perimeter (PSP), where physical access was controlled and monitored.	WECC_URE2 revoked the contractor's access to CCAs, thereby remediating the issue. The contractor was given cyber security training.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010525	CIP-004-3	R3	WECC_URE2 submitted three Self-Reports citing issues of CIP-004-3 R3, CIP-005-3 R1 and CIP-006-3 R2. CIP-004-3 R3 requires that entities ensure a personnel risk assessment (PRA) is completed prior to granting individuals electronic or physical access to Critical Cyber Assets (CCAs). CIP-005-3 R1 and CIP-006-3 R2 incorporate by reference CIP-004-3 R3, thereby requiring a PRA prior to any grant of access to Cyber Assets provisioning electronic access control and monitoring and Cyber Assets provisioning physical and access control and monitoring, respectively. WECC determined that WECC_URE2 granted a single contractor physical and electronic access to CCAs and Cyber Assets provisioning physical and electronic access control and monitoring. WECC determined that the contractor was granted access without first completing a PRA under CIP-004-1 R3. WECC also determined that the contractor was also granted access to Cyber Assets provisioning electronic and physical access control and monitoring in noncompliance with CIP-005-3 R1 and CIP-006-3 R2.	WECC 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 noncompliance stems from a single instance in which WECC_URE2 granted access to a contractor, before that contractor completed a PRA. The scope of the issue is, therefore, limited. The contractor had access for less than a twenty-four hour period. The contractor subsequently completed a PRA and was given access to Cyber Assets and CCAs. All CCAs and Cyber Assets were located within an Electronic Security Perimeter and Physical Security Perimeter. All access was logged and monitored.	WECC_URE2 terminated the contractor's electronic and physical access rights to CCAs thereby remediating the issue. The contractor subsequently completed a PRA and was given access to Cyber Assets and CCAs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010393	CIP-005-3a	R5	WECC_URE2 submitted a Self-Report citing possible noncompliance with CIP-005-3 R5. Specifically, WECC_URE2 reported that it failed to update documentation to reflect modification of network or controls within 90 calendar days of the change. WECC determined that WECC_URE2 added four Access Control and Monitoring (ACM) devices to the Electronic Security Perimeter (ESP). Per CIP-005-3 R5.2, WECC_URE2 was required to update ESP documentation to reflect this change within 90 days. WECC determined, however, that WECC_URE2 did not update ESP documentation to reflect this change in ESP controls until 397 days later when WECC_URE2 completed remediation activity.	WECC 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 four ACM devices were only used to monitor Critical Cyber Assets and Cyber Assets within the ESP during vulnerability assessments. Further, these devices were afforded a number of protections. Devices were contained within an ESP. Access to the ESP was controlled, monitored and logged during the issue period. The ESP was alarmed for cyber security events. Individuals with access to the devices completed cyber security training and personnel risk assessments (PRAs). The devices were physically secured within a Physical Security Perimeter (PSP). Physical access thereto was logged, controlled and monitored.	WECC_URE2 submitted a completed Mitigation Plan. In its Mitigation Plan, WECC_URE2 outlined the following actions completed: WECC_URE2 determined that the Network team that supports the EMS environment reviewed and updated the ESP drawings. Once these drawings were up to date with the current physical environment, WECC_URE2 proactively updates the documents whenever a relevant change to the environment exists.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010517	CIP-005-3a	R3	WECC_URE2 submitted two Self-Reports citing possible noncompliance with CIP-005-3 R3 and CIP-007-3 R6 at its backup control center (BUCC). Specifically, WECC_URE2 reported that it failed to review BUCC logs as required by CIP-005-3 R3.2 and CIP-007-3 R6.5. Pursuant to CIP-007 R6.5, WECC_URE2 is required to review logs of all system events. Similarly, under CIP-005-1 R3.2, WECC_URE2 is required to review Electronic Security Perimeter (ESP) access logs every 90 calendar days. WECC_URE2's BUCC review process under CIP-007-1 R6.5 required that all logs be maintained on BUCC primary servers. As of the mandatory and enforceable date of the Standard, however, system events associated with four Cyber Assets within the ESP were stored on BUCC backup servers. Consequently, WECC_URE2's review of system event logs did not include logs stored on the BUCC backup servers. Similarly, WECC_URE2's BUCC review process under CIP-005-3 R3.2 required that WECC_URE2 review BUCC ESP access logs maintained on primary servers every 90 days. In this case, WECC_URE2 reported that when it installed two BUCC ESP access points, it did not configure the devices to forward access logs to BUCC primary servers. Instead, access logs for the two devices were maintained on BUCC backup servers. WECC reviewed WECC_URE2's Self-Reports and logging documents. WECC determined that although WECC_URE2 did maintain logs under CIP-005-3 R3 and CIP-007-3 R6, WECC_URE2 failed to review these logs.	WECC 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 scope of the issues were limited to six devices associated with WECC_URE2's BUCC. Access logs and system event logs were being generated and maintained on backup servers. All devices within scope of both issues were secured within Physical Security Perimeters. Electronic and physical access to these devices was restricted to authorized personnel. Further, these devices were protected by layered security. Remote logical access to the devices was available only through the virtual private network (VPN). VPN logs were maintained and reviewed during the duration of the issue.	WECC_URE2 submitted a completed Mitigation Plan and Certification of Mitigation Plan Completion. The Mitigation Plan summarized mitigation action completed by WECC_URE2. WECC_URE2 installed new secondary log servers for both the System Control Center (SCC) and the BUCC. As part of this change, a spreadsheet was developed that listed each CIP-applicable Cyber Asset associated with the EMS (including the network devices at the BUCC). That list is derived from the list of CIP-applicable Cyber Assets maintained by the CIP program manager. A thorough review was completed to verify that each of those CIP-applicable Cyber Assets within the EMS environment that is capable of generating logs sends those logs to the appropriate primary and secondary log servers, as technically feasible. After reception of those logs are confirmed, WECC_URE2 ensured that each of the CIP-applicable Cyber Assets that is capable of generating logs associated with the EMS are included as "log sources" in pre-established alerting rules. These rules, at a minimum, include low and high logging thresholds. These alerts help to identify when logs sources either do not send logs within a certain timeframe (low-level threshold) or when they send too many logs within a certain timeframe (high-level threshold).
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012009457	CIP-006-3c	R5	WECC_URE2 submitted a Self-Certification citing possible noncompliance with CIP-006-3c R5. Specifically, WECC_URE2 disclosed that it failed to ensure 24 hours a day, seven days a week monitoring of physical access to a Physical Security Perimeter (PSP) for a period of approximately four hours and 22 minutes. WECC determined that there was a communication failure of physical access control panels at WECC_URE2's backup control center (BCC). Consequently, WECC_URE2 alarming at the BCC PSP was disabled. After a period of four hours and 22 minutes, WECC_URE2 security personnel discovered the failure and immediately dispatched onsite security personnel to monitor the PSP using human observation.	WECC 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 scope of the issue is limited to a single PSP for a period of four hours and 22 minutes. During the issue period, access to the PSP was controlled and logged through a card reader. After reviewing access logs, WECC_URE2 confirmed that there were no unauthorized access attempts that would have triggered alarming. Further, the BCC was not in operation during the issue period.	WECC_URE2 submitted a completed Mitigation Plan describing the following mitigation activities: 1. Incident review and training. Corporate security reviewed the sequence of events with the on-duty security personnel and provided guidance on response actions for alarms related to operational failures. The security supervisor also did a follow-up with personnel and provided direction on the importance and criticality of immediate response and notification of alarms related to CIP Assets; 2. Update to CIP alarm response protocol and recognition. Corporate security modified the designators of all CIP impacted components (node controllers, card readers) to include a CIP designation to better identify associated alarms. This provides a better visual cue to on-duty security personnel in order to react and respond to alarms related to CIP Assets. Corporate security also provided an update to the response protocol to all security personnel stressing the importance of notifying corporate security in a timely manner to ensure appropriate response and mitigation of CIP controls (physical access, monitoring, and logging) for all outages.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010518	CIP-007-1	R6	WECC_URE2 submitted two Self-Reports citing possible noncompliance with CIP-005-3 R3 and CIP-007-3 R6 at its backup bontrol benter (BUCC). Specifically, WECC_URE2 reported that it failed to review BUCC logs as required by CIP-005-3 R3.2 and CIP-007-3 R6.5. Pursuant to CIP-007 R6.5, WECC_URE2 is required to review logs of all system events. Similarly, under CIP-005-1 R3.2, WECC_URE2 is required to review Electronic Security Perimeter (ESP) access logs every 90 calendar days. WECC_URE2's BUCC review process under CIP-007-1 R6.5 required that all logs be maintained on BUCC primary servers. As of the mandatory and enforceable date of the Standard, however, system events associated with four Cyber Assets within the ESP were stored on BUCC backup servers. Consequently, WECC_URE2's review of system event logs did not include logs stored on the BUCC backup servers. Similarly, WECC_URE2's BUCC review process under CIP-005-3 R3.2 required that WECC_URE2 review BUCC ESP access logs maintained on primary servers every 90 days. In this case, WECC_URE2 reported that when it installed two BUCC ESP access points, it did not configure the devices to forward access logs to BUCC primary servers. Instead, access logs for the two devices were maintained on BUCC backup servers. WECC reviewed WECC_URE2's Self-Reports and logging documents. WECC determined that although WECC_URE2 did maintain logs under CIP-005-3 R3 and CIP-007-3 R6, WECC_URE2 failed to review these logs.	WECC 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 scope of the issues was limited to six devices associated with WECC_URE2's BUCC. Access logs and system event logs were being generated and maintained on backup servers. All devices within scope of both issues were secured within Physical Security Perimeters. Electronic and physical access to these devices was restricted to authorized personnel. Further, these devices were protected by layered security. Remote logical access to the devices was available only through the virtual private network (VPN). VPN logs were maintained and reviewed during the duration of the issue.	WECC_URE2 submitted a completed Mitigation Plan and Certification of Mitigation Plan Completion. The Mitigation Plan summarized mitigation action completed by WECC_URE2: WECC_URE2 installed new secondary log servers for both the system control center (SCC) and the BUCC. As part of this change, a spreadsheet was developed that listed each CIP-applicable Cyber Asset associated with the EMS (including the network devices at the BUCC). That list is derived from the list of CIP-applicable Cyber Assets maintained by the CIP program manager. A thorough review was completed to verify that each of those CIP-applicable Cyber Assets within the EMS environment that is capable of generating logs sends those logs to the appropriate primary and secondary log servers, as technically feasible. After reception of those logs are confirmed, WECC_URE2 ensured that each of the CIP-applicable Cyber Assets that is capable of generating logs associated with the EMS are included as "log sources" in pre-established alerting rules. These rules, at a minimum, include low and high logging thresholds. These alerts help to identify when logs sources either do not send logs within a certain timeframe (low-level threshold) or when they send too many logs within a certain timeframe (high-level threshold).
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010528	CIP-007-3	R5	WECC_URE2 submitted a Self-Report citing possible noncompliance with CIP-007-3 R5. Specifically,WECC_URE2 reported that access to a user account was granted to an individual without the approval of designated personnel as required by CIP-007-1 R5.1.1. Based on additional information disclosed by WECC_URE2, WECC determined that WECC_URE2 granted access to user accounts without the approval of designated personnel on three occasions. WECC determined that in each instance, a single individual was granted access to a user account without the approval of designated personnel. Further, WECC determined that in each instance, WECC_URE2 revoked access to the user account on the same day unapproved access was granted.	WECC 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 each instance spanned a period of 24 hours. Two of the individuals involved completed cyber security training and the personnel risk assessments prior to receiving user account access. Each of the three individuals in scope required access to the user accounts. The devices that could be accessed through the user accounts were all secured within an Electronic Security Perimeter (ESP) and Physical Security Perimeters (PSPs). All access to the Cyber Assets and Critical Cyber Assets was logged and monitored. The ESP and PSP were set to alarm security personnel in the event of unauthorized access attempts or security events.	WECC_URE2 revoked the individual's access to a user account after discovering that access had been granted without the requisite approval. WECC_URE2 revoked the individual's access to a user account after discovering that access had been granted without requisite approval. WECC_URE2 revoked the individual's access to a user account after discovering that access had been granted without requisite approval. WECC_URE2 retrained personnel on access procedures.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) Idaho Power Company (IPCO)	NCRXXXXX	WECC2012010738	CIP-005-1	R2	During a Compliance Audit of WECC_URE3, the Audit team determined that WECC_URE3 failed to display a warning banner (i.e., an appropriate use banner) on access points to Electronic Security Perimeters (ESP) for interactive access prior to login. Pursuant to the Standard, all attempts of interactive access must display an appropriate use banner upon access and prior to successful login. As documented in WECC_URE3's access point configuration files and as validated through physical observation during site visits, the access points have only defined the command which does not display the banner as part of the initial user access prior to login. Based on this, WECC determined WECC_URE3's configuration is incorrect for not displaying the appropriate use banner prior to login. WECC further determined WECC_URE3 could not demonstrate that the configuration for these access points had been correct since the mandatory compliance date of CIP-005-1.	WECC 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 because, WECC_URE3 has defined processes and procedures for granting access, which include strict access controls to Critical Cyber Assets. Additionally, WECC_URE3 has active monitoring and automatic alert mechanisms, as well as physical separation from external access through the use of firewall technology. Finally, WECC_URE3 did have appropriate use banners on the majority of its electronic access devices, however, in this instance, WECC_URE3 configured the devices to display the appropriate use banner after a user logged into the system and not upon all interactive access attempts.	WECC_URE3 configured the devices to display the appropriate use banner upon interactive access attempts. Specifically, WECC_URE3 configured the devices to display the appropriate use banner prior to access attempts. WECC_URE3 further maintains a document identifying the content of the banner.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010307	CIP-007-3	R3	During WECC_URE4's on-site compliance Audit, the WECC Audit Team reviewed compliance with CIP-007-3 R3. During the course of the Audit, the Audit Team discovered that WECC_URE4 failed to document the assessment of two security patches within 30 calendar days of availability. The Audit team reviewed the assessment of 35 applicable patches for WECC_URE4. Of the 35 security patches, two were reviewed and assessed later than 30 days. Specifically, the vendor released patches on for the identification of potential security vulnerabilities. WECC_URE4 received the patch information but failed to document the correct release date. Consequently, WECC_URE4 failed to assess and install the security patches until four days and seven days after the 30 day requirement had lapsed.	WECC 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 WECC_URE4 did establish and implement a security patch management program and a configuration management process for all system patches. The two security patches addressed herein were reviewed for applicability within a week after the 30 day requirement, and the Audit team determined that the assessment of security patches were up to date. The assets in scope are protected within WECC_URE4's Electronic Security Perimeters and Physical Security Perimeters, and have 24 hour a day logging and monitoring.	WECC_URE4 reviewed, assessed and installed the security patch applications. WECC_URE4's patch management process was reviewed and updated as follows: 1. The review of the Supervisory Control and Data Acquisition (SCADA) vendor patch report will no longer be considered during the assessment of security patches for applicability. 2. SCADA vendor patch reports will be referenced during the testing phase of the patch management process. 3. The documented results of patch management meetings will be reviewed and signed-off by two Emergency Management System (EMS) personnel. 4. The training of applicable staff on new/updated patch process.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2012009101	CIP-007-1	R4	WECC_URE5 submitted a Self-Report addressing possible noncompliance with CIP-007-1 R4. Specifically, WECC_URE5 reported that it failed to use anti-virus software or other malware prevention tools on 64 firewalls and 361 routers and switches within 50 Electronic Security Perimeters (ESPs). Upon further review, WECC_URE5 determined there are no anti-virus applications available for the operating systems associated with the Cyber Assets and, as a result, submitted two late-filed TFEs addressing technical infeasibility with CIP-007-1 R4.	WECC 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 WECC_URE5's noncompliance is limited given compensating measures that were in place prior to the due date on which all TFE requests were to originally be submitted to WECC. Specifically, the Cyber Assets are located in an ESP and have technical and procedural mechanisms for control of electronic access at all access points. Also, all devices are located within a Physical Security Perimeter (PSP) and have technical and procedural controls to manage physical access to the PSPs including 24 hour a day, seven day a week logging and monitoring of physical access. Additionally, WECC_URE5 requires username and passwords on all Critical Assets and uses a passive triggering mechanism to monitor any changes.	WECC_URE5 submitted a Mitigation Plan for CIP-007-1 R4. WECC_URE5 submitted two TFEs for the 425 assets in scope. WECC_URE5's plan requires the development and implementation of training for personnel supporting and maintaining assets in scope for NERC-CIP requirements. This training will ensure that the appropriate personnel have an appropriate understanding of TFEs that includes training on submission of timely TFEs. WECC approved the late filed TFEs associated with CIP-007-1 R4 network devices.

Document Accession #: 20120928-5322 Filed Date: 09/28/2012

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

September 28, 2012

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

Re: NERC FFT Informational Filing
FERC Docket No. RC12-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find, Fix, Track and Report[1] (FFT) in Attachment A regarding 41 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 75 possible violations[5] of 18 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 75 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.
[3] Attachment A is an Excel spreadsheet.
[4] *See* 18 C.F.R § 39.7(c)(2).
[5] For purposes of this document, each matter is described as a "possible violation," regardless of its procedural posture.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is appropriate disposition of these matters, and will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards.

Statement of Findings Underlying the FFT

The descriptions of the remediated issues and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval by NERC Enforcement staff, under delegated authority from the NERC Board of Trustees Compliance Committee (NERC BOTCC), of the findings reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), each Reliability Standard at issue in this FFT is identified in Attachment A.

Text of the Reliability Standards at issue in the FFT may be found on NERC's website at http://www.nerc.com/page.php?cid=2|20. For each respective remediated issue, the Reliability Standard Requirement at issue is listed in Attachment A.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the possible violations identified in Attachment A have been mitigated. The respective Registered Entity has submitted a certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, spot check, random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

[6] *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) ("March 15, 2012 CEI Order"); *see also North American Electric Reliability Standards Development and NERC and Regional Entity Enforcement*, 132 FERC ¶ 61,217 at P.218 (2010)(encouraging streamlined administrative processes aligned with the significance of the subject violations).
[7] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Resolution[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,[9] NERC Enforcement staff under delegated authority from the NERC BOTCC, approved the FFT based upon its findings and determinations, as well as its review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the remediated issues.

Notice of Completion of Enforcement Action

In accordance with section 5.10 of the CMEP, and the Commission's March 15, 2012 CEI Order, provided that the Commission has not issued a notice of review of a specific matter included in this filing, notice is hereby provided that, sixty-one days after the date of this filing, enforcement action is complete with respect to all remediated issues included herein and any related data holds are released only as to that particular remediated issue.

Pursuant to the Commission order referenced above, both the Commission and NERC retain the discretion to review a remediated issue after the above referenced sixty-day period if it finds that FFT treatment was obtained based on a material misrepresentation of the facts underlying the FFT matter. Moreover, to the extent that it is subsequently determined that the mitigation activities described herein were not completed, the failure to remediate the issue will be treated as a continuing possible violation of a Reliability Standard requirement that is not eligible for FFT treatment.

Request for Confidential Treatment of Certain Attachments

Certain portions of Attachment A include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain

[8] *See* 18 C.F.R § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010).

Reliability Standard possible violations and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the information in the attached documents is deemed "confidential" by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be included as Part of this FFT Informational Filing

The attachments to be included as part of this FFT Informational Filing are the following documents and material:

a) Find, Fix, Track and Report Spreadsheet, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this FFT:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

Handling these remediated issues in a streamlined process will help NERC, the Regional Entities, Registered Entities, and the Commission focus on improving reliability and holding Registered Entities accountable for the more serious violations of the mandatory and enforceable NERC Reliability Standards. Accordingly, NERC respectfully submits this FFT as an informational filing.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
rebecca.michael@nerc.net

cc: Entities listed in Attachment B

NERC

Attachment a

Find, Fix, Track and Report Spreadsheet (Included in a Separate Document)

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR SEPTEMBER 2012
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

Stacy Dochoda*
President and Chief Executive Officer
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
sdochoda@frcc.com

Linda Campbell*
VP and Executive Director Standards & Compliance
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
lcampbell@frcc.com

Barry Pagel*
Director of Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 690
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5648 – facsimile
bpagel@frcc.com

FOR MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Director of Regulatory Affairs and Enforcement
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1708
se.patrick@midwestreliability.org

FOR NPCC:

Walter Cintron*
Manager, Compliance Enforcement
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
wcintron@npcc.org

Edward A. Schwerdt*
President and Chief Executive Officer
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
eschwerdt@npcc.org

Stanley E. Kopman*
Assistant Vice President of Compliance
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
skopman@npcc.org

FOR RFC:

Robert K. Wargo*
Director of Analytics & Enforcement
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
bob.wargo@rfirst.org

L. Jason Blake*
General Counsel
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
jason.blake@rfirst.org

Megan E. Gambrel*
Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
megan.gambrel@rfirst.org

Michael D. Austin*
Managing Enforcement Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
mike.austin@rfirst.org

FOR SERC:

John R. Twitchell*
VP and Chief Program Officer
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8205
(704) 357-7914 – facsimile
jtwitchell@serc1.org

Marisa A. Sifontes*
General Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7775
(704) 357-7914 – facsimile
msifontes@serc1.org

Maggie A. Sallah*
Senior Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7778
(704) 357-7914 – facsimile
msallah@serc1.org

James M. McGrane*
Legal Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7787
(704) 357-7914 – facsimile
jmcgrane@serc1.org

Andrea B. Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

FOR SPP RE:

Ron Ciesiel*
General Manager
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1730
(501) 821-8726 – facsimile
rciesiel.re@spp.org

Joe Gertsch*
Manager of Enforcement
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1672
(501) 821-8726 – facsimile
jgertsch.re@spp.org

Machelle Smith*
Paralegal & SPP RE File Clerk
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1681
(501) 821-8726 – facsimile
spprefileclerk@spp.org

FOR TEXAS RE:

Susan Vincent*
General Counsel
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4922
(512) 233-2233 – facsimile
susan.vincent@texasre.org

Rashida Caraway*
Manager, Compliance Enforcement
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4977
(512) 233-2233 – facsimile
rashida.caraway@texasre.org

FOR WECC:

Mark Maher*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(360) 713-9598
(801) 582-3918 – facsimile
Mark@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6855
(801) 883-6894 – facsimile
CWhite@wecc.biz

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7674
(801) 883-6894 – facsimile
RArredondo@wecc.biz

Christopher Luras*
Director of Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RC12-___-000

NOTICE OF FILING
September 28, 2012

Take notice that on September 28, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding forty-one (41) Registered Entities in eight (8) Regional Entity footprints.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211, 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. Such notices, motions, or protests must be filed on or before the comment date. On or before the comment date, it is not necessary to serve motions to intervene or protests on persons other than the Applicant.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original and 14 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, D.C. 20426.

This filing is accessible on-line at http://www.ferc.gov, using the "eLibrary" link and is available for review in the Commission's Public Reference Room in Washington, D.C. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Document Content(s)