September 30, 2011

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of violations[3] of BAL-004-0 Requirement (R) 3, CIP-003-1 R1, CIP-004-1 R2/2.3 and R4, CIP-007-1 R1 and R2, TOP-004-2 R1, TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1. According to the Settlement Agreement, URE neither admits nor denies that its actions or non-actions constitute violations of the Reliability Standards, but does agree and stipulate to the facts of the violations as laid out in the Settlement Agreement and has agreed to the assessed penalty of two hundred twenty-five thousand dollars ($225,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

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

terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201001947, WECC201001965, WECC201001966, WECC201001967, WECC201001964, WECC201002011, WECC201001902, WECC201002026, WECC201002027, WECC201002028 and WECC201002029 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on June 21, 2011, by and between WECC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2007), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	VSL	Total Penalty ($)
WECC	Unidentified Registered Entity	NOC-914	WECC201001947	BAL-004-0	3/3.1	Lower[4]	Lower	225,000
			WECC201001965	CIP-003-1[5]	1	Lower[6]	Severe	

[4] BAL-004-0 R3 has a "Medium" Violation Risk Factor (VRF); R3.1 and R3.2 each have a "Lower" VRF.
[5] CIP-003-1 was enforceable from July 1, 2008 through March 31, 2010. CIP-003-2 was enforceable from April 1, 2010 through September 1, 2010. The subsequent version does not change the language of the original NERC Reliability Standard and its requirements substantively. For consistency in this filing, the original NERC Reliability Standard, CIP-003-1, is used throughout.
[6] CIP-003-1 R1 has a "Medium" VRF; CIP-003-1 R1.1, R1.2 and R1.3 each have a "Lower" VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

			WECC201001966	CIP-004-1	2/2.3	Lower[7]	Severe	
			WECC201001967	CIP-004-1	4	Lower[8]	N/A[9]	
			WECC201001964	CIP-007-1	1	Medium[10]	N/A[11]	
			WECC201002011	CIP-007-1	2	Medium	N/A	
			WECC201001902	TOP-004-2	1	High	High	
			WECC201002026	TPL-001-0.1	1	High[12]	Severe	
			WECC201002027	TPL-002-0[13]	1	High[14]	Severe	
			WECC201002028	TPL-003-0[15]	1	High[16]	Severe	
			WECC201002029	TPL-004-0	1	Medium	Severe	

[7] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; CIP-004-1 R2.1, R2.2 and R2.2.4 each have a "Medium" VRF.
[8] CIP-004-1 R4 and R4.1 each have a "Lower" VRF; CIP-004-1 R4.2 has a "Medium" VRF.
[9] At the time of this violation, no VSL was in effect for CIP-004-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.
[10] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; CIP-007-1 R1.2 and R1.3 each have a "Lower" VRF.
[11] At the time of the violations, no VSLs were in effect for CIP-007-1 R1 and R2. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.
[12] TPL-001-0.1 R1 has a "High" VRF and all its sub-requirements each have a "Medium" VRF.
[13] TPL-002-0 was enforceable from June 18, 2007 through April 22, 2010. TPL-002-0a is the current enforceable version of the Standard as of April 23, 2010. The subsequent interpretation added Appendix 1 and only changes the meaning of R1.3.2 and R1.3.12, but does not change the language of the original NERC Reliability Standard and its requirements. For consistency in this filing, the original NERC Reliability Standard, TPL-002-0, is used throughout.
[14] TPL-002-0 R1 has a "High" VRF and all its sub-requirements each have a "Medium" VRF.
[15] TPL-003-0 was enforceable from June 18, 2007 through April 22, 2010. TPL-003-0a is the current enforceable version of the Standard as of April 23, 2010. The subsequent interpretation added Appendix 1 and only changes the meaning of R1.3.2 and R1.3.12, but does not change the language of the original NERC Reliability Standard and its requirements. For consistency in this filing, the original NERC Reliability Standard, TPL-003-0, is used throughout.
[16] TPL-003-0 R1 has a "High" VRF and all its sub-requirements each have a "Medium" VRF.

BAL-004-0 R3

The purpose of Reliability Standard BAL-004-0 provides: "The purpose of this standard is to ensure that Time Error Corrections are conducted in a manner that does not adversely affect the reliability of the Interconnection."

BAL-004-0 R3 provides:

> R3. Each Balancing Authority, when requested, shall participate in a Time Error Correction by one of the following methods:
>
> > R3.1. The Balancing Authority shall offset its frequency schedule by 0.02 Hertz, leaving the Frequency Bias Setting normal; or
> >
> > R3.2. The Balancing Authority shall offset its Net Interchange Schedule (MW) by an amount equal to the computed bias contribution during a 0.02 Hertz Frequency Deviation (i.e.20% of the Frequency Bias Setting).

BAL-004-0 R3.1 has a "Lower" VRF.

URE self-reported a violation of BAL-004-0 R 3 to WECC for URE's failure to offset its frequency schedule by 0.02% as requested by the Reliability Coordinator (RC) during a manual Time Error Correction (TEC).[17]

The RC requested URE to participate in a manual TEC effective 0:00 Pacific Time (PT) stating that the time error was 5.014 seconds. The request specifically asked Balancing Authorities to schedule frequency to 59.98 Hz. As requested, URE set its frequency to 59.98 Hz and began participating in the TEC event at 0:00 PT. URE initiated the TEC at 59.98 Hz and left the Frequency Bias Setting[18] on "normal," as required by the Standard. At 4:38:13 PT, URE's TEC automatically switched to "off" when

[17] *The NERC Glossary of Terms Used in Reliability Standards* defines "Time Error Correction" as an "offset to the Interconnection's scheduled frequency to return the Interconnection's Time Error to a predetermined value."
[18] *The NERC Glossary of Terms Used in Reliability Standards* defines "Frequency Bias Setting" as a "value, usually expressed in MW/0.1 Hertz, set into a Balancing Authority ACE algorithm that allows the Balancing Authority to contribute its frequency response to the Interconnection.

the time error[19] reached 0.00 seconds, and 24 seconds later, URE's TEC switched to "auto" to continue participating in the TEC event. Configuration was set such that when the error hit 0.00, URE's frequency auto switched when the time error went from positive to negative time accumulation. At this point, URE's TEC frequency automatically switched to 60.02 Hz because the time error had switched from a positive to a negative time accumulation.

WECC determined that URE had a violation of BAL-004-0 R3 because for approximately 82 minutes during the TEC, URE set its frequency schedule to 60.02 Hz, counter to the request that URE's frequency be scheduled at 59.98 Hz during the TEC.

WECC determined the duration of the violation to be the 82 minutes when URE had a frequency schedule of 60.02 Hz.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because URE's frequency automatically switched to 60.02 Hz only after the Time Error went from 5.014 seconds to zero seconds (*i.e.*, no error). Each Balancing Authority in the Western Interconnection participated in this TEC and URE's contribution to TEC from a generation standpoint, relative to the Interconnection, is small. Finally, URE's frequency schedule was incorrect for only a portion of the TEC.

CIP-003-1 R1

The purpose of Reliability Standard CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities [20] have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009." (Footnote added.)

CIP-003-1 R1 provides in pertinent part:

[19] *The NERC Glossary of Terms Used in Reliability Standards* defines "Time Error" as the "difference between the Interconnection time measured at the Balancing Authority (ies) and the time specified by the National Institute of Standards and Technology. Time Error is caused by the accumulation of Frequency Error over a given period." "Frequency Error" is defined as the "difference between the actual and scheduled frequency."

[20] Within the text of Standard CIP-003, CIP-004, and CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

CIP-003-1 R1 has a "Lower" VRF.

During a CIP Spot Check, WECC identified a violation of Reliability Standard CIP-003-1 R1 for URE's failure to provide evidence that its cyber security policy addressed all requirements in Standards CIP-002 through CIP-009, failed to include provisions for emergency situations in its cyber security policy, and failed to provide evidence that it made its cyber security policy readily available to all vendor personnel.

During the Spot Check, the Spot Check team reviewed multiple versions of URE's cyber security policy for CIP-003 and CIP-003 cyber security policy crosswalk. WECC determined that URE had a violation of CIP-003-1 R1 because the earlier version documents did not identify CIP-007-1 R7, CIP-007-1 R9 and CIP-008-1 R2, and did not include provisions for emergency situations. The later version associated crosswalk document did not identify CIP-002-1 R2, CIP-002-1 R3, CIP-002-1 R4, CIP-005-1 R4, CIP-006-1 R5, CIP-006-1 R6, CIP-007-1 R6, CIP-007-1 R8, CIP-007-1 R9, CIP-009-1 R2, CIP-009-1 R3, CIP-009-1 R4 and CIP-009-1 R5.

The Spot Check team then reviewed URE's subsequent cyber security policy and the associated crosswalk document, as well as the cyber security policy that was in effect through the start of the Spot Check and the associated crosswalk document. The Spot Check team determined both versions addressed the requirements in Standards CIP-002 through CIP-009, including provisions for emergency situations, was readily available to URE personnel, and that URE conducted an annual review including URE's senior manager's approval.

The Spot Check team submitted a data request to URE specifically asking for "additional evidence regarding the cyber security policy being readily available to all personnel from July 2008 to present."

In response to the data request, URE provided evidence that its cyber security policy was readily available to its employees. URE did clarify that one vendor with controlled access to URE's virtual private network (VPN) did not receive URE's cyber security policy. URE failed to make its cyber security policy available to its contracted vendor with access to or responsibility for Critical Cyber Assets (CCAs).

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE mitigated the instant violation.

WECC determined that this violation did not pose a serious or substantial risk to the reliability of the BPS because URE provided training to its personnel and the contracted vendor who did not receive the policy which covered all of the cyber security requirements, including those missing from the various versions of its cyber security policy.

CIP-004-1 R2/2.3

The purpose of Reliability Standard CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R2 provides in pertinent part:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> ****
>
> R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

CIP-004-1 R2.3 has a "Lower" VRF.

WECC notified URE that WECC would be performing a Spot Check at URE's office. URE self-reported a violation of CIP-004-1 R2.3 to WECC for URE's failure to conduct annual training in 2009 for 17% (62 out of 380) of URE employees with authorized cyber or unescorted physical access to CCAs.

URE discovered the violation of CIP-004-1 R2.3 while preparing for the Spot Check. URE had failed to provide annual cyber security training to 69 employees with authorized cyber or authorized unescorted physical access to CCAs. Upon discovering this issue of noncompliance, URE gave the annual security training to 62 of the 69 employees, with the remaining seven employees no longer having access to CCAs. WECC determined that URE did not have documentation (*e.g.*, date the training was completed and attendance records) that it conducted training for approximately 17% (62 out of 380) of URE personnel with authorized cyber or authorized unescorted physical access to CCAs.

WECC determined the duration of the violation to be from January 1, 2009, when URE exceeded the annual timeframe for security training, through April 10, 2010, when URE mitigated the instant violation.

WECC determined that this violation posed a moderate risk to the reliability of the BPS because a violation of this standard may lead to cyber security oversights and cyber security incidents resulting in potential security compromise of CCAs. This violation did not pose a serious or substantial risk to the BPS because the URE personnel who failed to receive cyber security training in 2009 did receive initial CIP cyber security training in 2008 and participated in quarterly cyber security reviews. URE's training program did not change substantively from 2008 to 2009.

CIP-004-1 R4

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible

> Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
>
> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" VRF.

During the Spot Check, WECC also identified a violation of Reliability Standard CIP-004-1 R4 for URE's failure to include certain personnel's specific electronic and physical access rights to CCAs and failure to conduct quarterly reviews of the list of URE personnel with authorized cyber or unescorted physical access rights to CCAs.

During the Spot Check, the Spot Check team reviewed URE's CCA user access management procedures, CCA user access quarterly review procedures, quarterly review matrix, and CCA user access revocation procedures. The Spot Check team determined URE maintained a list of personnel with authorized cyber or authorized unescorted physical access to CCAs. WECC determined that URE did not include specific electronic and physical access rights to CCAs as required by CIP-004-1 R4. URE also could not demonstrate the specific electronic access rights or roles for certain URE personnel during the same time period. Further, WECC determined that from URE did not demonstrate that it conducted quarterly reviews of personnel who have unescorted physical or cyber access to CCAs as required by CIP-004-1 R4.1.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE mitigated the instant violation.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The violation posed a moderate risk because the failure to maintain specific electronic access rights or roles for individual personnel could lead to unauthorized system use based on legacy system access. In addition, URE failed to conduct quarterly reviews of personnel who have unescorted physical or cyber access to CCAs therefore failing to strictly monitor and maintain access rights. The violation did not pose a serious or substantial risk because URE maintained a list of personnel with authorized cyber or unescorted physical access to CCAs and therefore had review and procedural controls in place which were effective.

CIP-007-1 R1

The purpose of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides in pertinent part:

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

CIP-007-1 R1 has a "Medium" VRF.

URE submitted its semiannual CIP Self-Certification stating that it was only "Substantially Compliant" with CIP-007-1 R1 because of URE's failure to (1) create, implement, and maintain cyber security test procedures in a manner that minimized adverse effects on URE's production system or its operation,

(2) document that testing is performed in a manner that reflects the production environment, and (3) document test results.

The Spot Check team conducted interviews with URE personnel regarding a CIP data request form that indicated its change control documentation was incomplete. During the interviews, URE personnel stated that URE only had functional test procedures (*i.e.*, operational testing, not cyber security testing). WECC determined that URE failed to create, implement, and maintain cyber security test procedures to ensure that signification changes to Cyber Assets within the Electronic Security Perimeter (ESP) do not adversely affect existing cyber controls.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE mitigated the instant violation.

WECC determined that this violation posed a moderate risk to the reliability of the BPS because without the test procedures prescribed in this requirement, new Cyber Assets or significant changes to existing Cyber Assets increases the likelihood that existing security controls fail over time. The expected or designed configuration of such controls will drift from the baseline as URE changes or adds to its system. This violation did not pose a serious or substantial risk to the BPS because URE did have functional test procedures and therefore URE conducted operational testing. Such testing would alert URE if changes or new assets affected the operation of a cyber asset.

CIP-007-1 R2

CIP-007-1 R2 provides in pertinent part:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF.

URE submitted its semiannual CIP Self-Certification stating that it was only "Substantially Compliant" with CIP-007-1 R2 because of URE's failure to establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled.

A WECC SME reviewed URE's Self-Certification and CIP data request form. The SME determined that, without testing its baselines for ports and services, URE was not aware which ports and services were required for normal and emergency operations and which ports and services it could or should disable (*i.e.*, the ports and services not required for normal and emergency situations). Because URE did not test its baselines for ports and services, it could not establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled; such a failure violates CIP-007-1 R2.

WECC determined the duration of the violation to be from the date the Standard became enforceable, through when URE mitigated the instant violation.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS because URE had established change control and change management procedures during the violation period which included thorough operational testing and documentation. The CCA related to this violation resides in a secure, low change environment. Further, the production control system is on a closed network, which is running no routable protocol outside of the ESP, minimizing exposure to cyber attack.

TOP-004-2 R1

The purpose of Reliability Standard TOP-004-2 provides: "To ensure that the transmission system is operated so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single Contingency and specified multiple Contingencies."

TOP-004-2 R1 provides: "Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs)."

TOP-004-2 R1 has a "High" VRF.

URE self-reported a violation of TOP-004-2 R1 to WECC because URE exceeded the System Operating Limit (SOL) on a path for more than 30 minutes.

URE was informed by another entity that a line went out of service. Upon inputting this outage into its path SOL calculator, URE de-rated the path to the stability limit. After learning that the SOL for the path had been exceeded, URE immediately started coordinating with the other entity to take actions to decrease the path flow below its SOL.

The RC contacted URE about the SOL overload. URE informed the RC about the path being de-rated, which was caused by the outage of the line, and that this line was expected to be back in service shortly. The RC recommended that URE start ramping the units down, assuming the outage of the line would not be brought to service shortly. Upon this direction, URE began reducing generation to mitigate the flow of the path.

The RC issued URE a directive to reduce flow to within the SOL. URE began decreasing generation to comply with the RC directive and continued coordinating with the RC. The line was restored and the path rating was increased. The SOL for the path was exceeded for more than 30 minutes.

WECC determined the duration of the violation to be more than 30 minutes on a single day.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the transmission element involved with this violation is a transmission line that constitutes a WECC path. Failure to operate this path to its correct limit could overload other lines, leading to expanding outages and possible system instability. In this case, the line was operated 9% over its SOL for more than 30 minutes.

Although risk to the BPS for operating above limits could have severe consequences, in this case there are significant mitigating factors. Loss of the line would have automatically engaged the URE's contingency arming system. The contingency arming system mitigates disturbances by tripping one or two generating units. Additionally, there is back-up protection to the contingency arming system in the form of power relays. In the event of the loss of the line without appropriate function of the contingency arming system, the relays operate to separate the system from the URE system to prevent

further jeopardy to the system. Other relays provide back-up protection to the contingency arming system, and operate to separate the system from the URE system, thereby reducing potential constraints on the system if necessary. Furthermore, URE was taking action to reduce generation and curtailing schedules to reduce flow on the path during the event, although it did not bring the line under its SOL before the line was returned to service.

TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1[21]

The purpose of Reliability Standards TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 provide: "System simulations and associated assessments are needed periodically to ensure that reliable systems are developed that meet specified performance requirements with sufficient lead time, and continue to be modified or upgraded as necessary to meet present and future system needs."

TPL-001-0.1 R1

TPL-001-0.1 R1 provides:

> R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non- recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I. To be considered valid, the Planning Authority and Transmission Planner assessments shall:
>
> > R1.1. Be made annually.
> >
> > R1.2. Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.
> >
> > R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category A of Table 1 (no contingencies). The specific elements

[21] There are no substantive differences between the purpose statements of these Standards.

selected (from each of the following categories) shall be acceptable to the associated Regional Reliability Organization(s). [22]

R1.3.1. Cover critical system conditions and study years as deemed appropriate by the entity performing the study.

R1.3.2. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.3. Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.

R1.3.4. Have established normal (pre-contingency) operating procedures in place.

R1.3.5. Have all projected firm transfers modeled.

R1.3.6. Be performed for selected demand levels over the range of forecast system demands.

R1.3.7. Demonstrate that system performance meets Table 1 for Category A (no contingencies).

R1.3.8. Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category A.

(Footnote added.)

[22] Consistent with applicable FERC precedent, the term "Regional Reliability Organization" in this context refers to WECC.

TPL-002-0 R1

TPL-002-0 R1 provides:

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (nonrecallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I. To be valid, the Planning Authority and Transmission Planner assessments shall:

R1.1. Be made annually.

R1.2. Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.

R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category B of Table 1 (single contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).

R1.3.1. Be performed and evaluated only for those Category B contingencies that would produce the more severe System results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.

R1.3.2. Cover critical system conditions and study years as deemed appropriate by the responsible entity.

R1.3.3. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.4. Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.

R1.3.5. Have all projected firm transfers modeled.

R1.3.6. Be performed and evaluated for selected demand levels over the range of forecast system Demands.

R1.3.7. Demonstrate that system performance meets Category B contingencies.

R1.3.8. Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.

R1.3.10. Include the effects of existing and planned protection systems, including any backup or redundant systems.

R1.3.11. Include the effects of existing and planned control devices.

R1.3.12. Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category B of Table I.

R1.5. Consider all contingencies applicable to Category B.

TPL-003-0 R1

TPL-003-0 R1 provides:

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard. To be valid, the Planning Authority and Transmission Planner assessments shall:

R1.1. Be made annually.

R1.2. Be conducted for near-term (years one through five) and longer-term (years six through ten) planning horizons.

R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category C of Table 1 (multiple contingencies). The specific elements selected (from each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).

R1.3.1. Be performed and evaluated only for those Category C contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.

R1.3.2. Cover critical system conditions and study years as deemed appropriate by the responsible entity.

R1.3.3. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.4. Be conducted beyond the five-year horizon only as needed to address identified marginal conditions that may have longer lead-time solutions.

R1.3.5. Have all projected firm transfers modeled.

R1.3.6. Be performed and evaluated for selected demand levels over the range of forecast system demands.

R1.3.7. Demonstrate that System performance meets Table 1 for Category C contingencies.

R1.3.8. Include existing and planned facilities.

R1.3.9. Include Reactive Power resources to ensure that adequate reactive resources are available to meet System performance.

R1.3.10. Include the effects of existing and planned protection systems, including any backup or redundant systems.

R1.3.11. Include the effects of existing and planned control devices.

R1.3.12. Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those Demand levels for which planned (including maintenance) outages are performed.

R1.4. Address any planned upgrades needed to meet the performance requirements of Category C.

R1.5. Consider all contingencies applicable to Category C.

TPL-004-0 R1

TPL-004-0 R1 provides:

R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I. To be valid, the Planning Authority's and Transmission Planner's assessment shall:

R1.1. Be made annually.

R1.2. Be conducted for near-term (years one through five).

R1.3. Be supported by a current or past study and/or system simulation testing that addresses each of the following categories, showing system performance following Category D contingencies of Table I. The specific elements selected (from within each of the following categories) for inclusion in these studies and simulations shall be acceptable to the associated Regional Reliability Organization(s).

R1.3.1. Be performed and evaluated only for those Category D contingencies that would produce the more severe system results or impacts. The rationale for the contingencies selected for evaluation shall be available as supporting information. An explanation of why the remaining simulations would produce less severe system results shall be available as supporting information.

R1.3.2. Cover critical system conditions and study years as deemed appropriate by the responsible entity.

R1.3.3. Be conducted annually unless changes to system conditions do not warrant such analyses.

R1.3.4. Have all projected firm transfers modeled.

R1.3.5. Include existing and planned facilities.

R1.3.6. Include Reactive Power resources to ensure that adequate reactive resources are available to meet system performance.

R1.3.7. Include the effects of existing and planned protection systems, including any backup or redundant systems.

R1.3.8. Include the effects of existing and planned control devices.

R1.3.9. Include the planned (including maintenance) outage of any bulk electric equipment (including protection systems or their components) at those demand levels for which planned (including maintenance) outages are performed.

R1.4. Consider all contingencies applicable to Category D.

TPL-001-0.1 R1, TPL-002-0 R1 and TPL-003-0 R1 each have a "High" VRF; TPL-004-0 R1 has a "Medium" VRF.

URE self-reported violations of TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 to WECC because of URE's failure to finalize documentation for a new assessment within the required timeframe.

WECC reviewed the Self-Report, conducted a phone interview with URE's Reliability Standards compliance officer, and requested URE's previous annual assessment. URE submitted a valid 2008 annual assessment. URE did not complete its 2009 annual assessment until 2010, and therefore did not finalize an annual assessment in the required timeframe. WECC determined that URE had violations of TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 because URE could not demonstrate that its portion of the interconnected transmission system is planned such that: with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services at all demand levels over the range of forecast system demands, under the conditions defined in the Reliability Standards.

WECC exercised its discretion under Section 3.10 of the NERC Sanction Guidelines to determine that the violations of TPL-001-0 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 were "related to a single act or common incidence of non-compliance" for which WECC would assess "a single aggregate penalty."[23]

WECC determined the duration of the violations to be from the date the assessments were due before, through when URE mitigated the instant violations.

WECC determined that these violations posed a minimal and not a serious or substantial risk to the reliability of the BPS because URE did timely complete its annual progress report, which summarizes the studies that would ultimately create a valid annual assessment. URE provided its annual progress report to the WECC Technical Studies Subcommittee. The studies prepared for the annual progress report and for the valid annual assessment did not identify areas of concern; the 2009 studies did not identify any changes (*e.g.*, move up in-service dates) to projects identified as necessary in the 2008 valid assessment. Finally, URE did demonstrate through its assessment, and in its earlier annual progress report, that its portion of the interconnected transmission system is planned such that it can be operated to supply projected customer demands and projected Firm Transmission Services at all demand levels over the range of forecast system demands.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred twenty-five thousand dollars ($225,000) for the referenced violations. In reaching this determination, WECC considered the following factors: (1) URE took voluntary corrective action with respect to each of the violations, which WECC considered as a mitigating factor, (2) URE was cooperative throughout WECC's evaluation of its compliance with the Reliability Standards and the enforcement process, (3) WECC applied mitigating credit for the seven self-reported violations contained herein, (4) WECC considered URE's internal compliance program (ICP) and improvements in its culture of compliance as a mitigating factor when assessing the penalty, (5) WECC considered that there was no failure by URE to comply with applicable compliance directives, (6) there was no evidence of an intentional violation or an attempt by URE to conceal a violation, and (7) WECC exercised its discretion under Section 3.10 of the NERC Sanction Guidelines and determined the violations of TPL-001-0 R1, TPL-002-0 R1, TPL-003-0 R1

[23] "[I]n cases where multiple violations are related to a single act or common incidence of noncompliance, the regional entity will generally issue a single aggregate penalty bearing a reasonable relationship to the aggregate of the related violations." NERC Sanction Guidelines (January 15, 2008).

and TPL-004-0 R1 were "related to a single act or common incidence of non-compliance" for which WECC would assess "a single aggregate penalty."

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred twenty-five thousand dollars ($225,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[24]

BAL-004-0 R3
URE's Mitigation Plan to address its violation of BAL-004-0 R3 was submitted to WECC on May 28, 2010 with a proposed completion date of June 30, 2010. The Mitigation Plan was accepted by WECC on June 17, 2010 and approved by NERC on June 30, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on July 8, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Conduct meetings with URE BPS operating personnel to analyze the circumstances of the event and provide documentation of the meeting to WECC.
2. Re-evaluate processes and improve procedures as may be applicable related to the TEC based on what is learned from the analysis of the event, and provide documentation of the improved procedures to WECC.
3. Enhance displays and create additional alarms (when in Auto mode) to improve the awareness to the operator, and provide documentation of these enhancements to WECC.

URE certified on June 30, 2010 that the above Mitigation Plan requirements were completed on June 25, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Memo summarizing technical meeting.
2. Bulk operations guide.
3. Training program.
4. Training roster.

[24] *See* 18 C.F.R § 39.7(d)(7).

5. Three screen shots showing URE's enhanced displays and new alarms.

On January 31, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 25, 3011 and that URE was in compliance with BAL-004-0 R3.

CIP-003-1 R1

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted to WECC on October 21, 2010 with a proposed completion date of April 15, 2010. The Mitigation Plan was accepted by WECC on January 25, 2011 and approved by NERC on March 7, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 10, 2011 in accordance with FERC orders.

Under the Mitigation Plan:

1. URE sent its cyber security policy to the vendor that had not previously received it.
2. The 2010 version of the cyber security policy and subsequent versions fully list all the requirements and sub-requirements of Standards CIP-002 through CIP-009, clearly list cyber security emergency provisions, and specifically state URE will provide its cyber security policy to vendors and contractors who are granted controlled remote cyber access.

URE certified on November 18, 2010 that the above Mitigation Plan requirements were completed on April 15, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's cyber security policy demonstrates URE's commitment to implement and comply with all NERC CIP-002 through CIP-009 requirements.
2. URE's cyber security policy clearly lists URE's cyber security emergency provisions.
3. URE's NERC CIP-003 compliance program specifically states that URE will provide its cyber security policy to vendors and contractors who are granted controlled remote cyber access.

On February 8, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on April 15, 2010 and that URE was in compliance with CIP-003-1 R1.

CIP-004-1 R2/2.3

URE's Mitigation Plan to address its violation of CIP-004-1 R2.3 was submitted to WECC on May 3, 2010 stating it had been completed on April 22, 2010. The Mitigation Plan was accepted by WECC on August

2, 2010 and approved by NERC on August 27, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on August 27, 2010 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Give annual security training to 62 of the 69 employees and generated verification lists.
2. Provide refresher training to its facility managers and its access list managers wherein URE clarified its cyber security training procedures.
3. Reiterate cyber security procedures training at monthly meetings with facility managers.

URE certified on May 4, 2010 that the above Mitigation Plan requirements were completed on April 22, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. List of the 62 employees in question and the dates they received the required annual training, as well as the seven employees that no longer required access.
2. List of 40 of the 62 employees that received the web based annual training.
3. Attendance sheets with remaining 22 employees receiving classroom training in 2010.
4. Agenda, meeting roster and minutes of the meeting with facility managers.
5. Annual CIP cyber security training procedure document.
6. URE's cyber security access list database printouts.

On August 11, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on April 10, 2010 and that URE was in compliance with CIP-004-1 R2.3.

CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to WECC on October 21, 2010, stating it had been completed on June 6, 2009. The Mitigation Plan was accepted by WECC on February 1, 2011 and approved by NERC on March 7, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on March 10, 2011 in accordance with FERC orders.

Under the Mitigation Plan:

1. URE performed training for its control center and emergency dispatch facility manager and designees and other facility managers and designees throughout the quarter in order to re-

emphasize the obligations and responsibilities to maintain CCA personnel access lists and comply with all requirements of NERC Standard CIP-004-1 R4.

2. A manager's directive was issued listing the specific requirements of NERC Standard CIP-004-1 R4 and detailed the obligations and responsibilities for power system facility managers to maintain those lists. The manager's directive was specifically distributed to the control center and emergency dispatch facility manager and designees.
3. Facility managers confirmed by email their review of access lists by the end of the second quarter.

URE certified on November 18, 2010 that the above Mitigation Plan requirements were completed on June 6, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Contents of training for the control center and emergency dispatch facility manager and designees.
2. Attendance list for the training.
3. Attendance lists for the training performed for all the facility managers and designees during the second quarter of 2009.
4. Follow-up e-mail (1) requesting the facility managers and designees review the new access list procedures covered in the training sessions, and (2) announcing that a new reformatted CCA personnel access list database is ready for use.
5. Manager's directive.
6. E-mail confirmation of quarterly review of the control center and emergency dispatch personnel access lists during the second quarter of 2009.
7. E-mail announcing that on June 5, 2009, the new reformatted web-based management of the CCA personnel access list database was in production and ready for use.
8. E-mail directed to the control center and emergency dispatch facility managers and designees that they have been granted full access to the database.
9. Screen shots of the web-based management database.

On February 8, 2011, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 6, 2010 and that URE was in compliance with CIP-004-1 R4.

CIP-007-1 R1 and R2

URE's Mitigation Plan to address its violation of CIP-007-1 R1 and R2 was submitted to WECC on March 8, 2010 stating it had been completed on January 28, 2010. The Mitigation Plan was accepted by WECC on June 14, 2010 and approved by NERC on July 8, 2010. The Mitigation Plan for this violation was submitted as non-public information to FERC on July 8, 2010 in accordance with FERC orders.

Under the Mitigation Plan:

1. Before the formal baselines were established, inbound ports and services to access points in the system for CCAs located at the control center were reviewed after a change was implemented.
2. URE reviews a list of inbound ports and services when a change has been implemented on a CCA and then turn offs any additional ports and services that were opened during the implementation of that change.
3. To avoid potential for human error, URE installed the software at the control center to track change configurations and change management.

URE certified on March 8, 2010 that the above Mitigation Plan requirements were completed on January 28, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's 83 documents including test results, test procedures and documented testing was performed reflecting the production environment.[25]
2. E-mail with the control center baseline confirmation.

On June 25, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on January 8, 2010 for R1 and January 28, 2010 for R2 and that URE was in compliance with CIP-007-1 R1 and R2.

TOP-004-2 R1

URE's Mitigation Plan to address its violation of TOP-004-2 R1 was submitted to WECC with a proposed completion date of June 18, 2010. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

[25] For a full list of the 83 documents, *see* Settlement Agreement at pg.13-15.

1. Coordinate with another entity's operating personnel to agree on a procedure to avoid any delays on communicating events that may affect the operation of the identified path, and provide documentation of the coordination and procedure to WECC.
2. Coordinate a meeting with all URE BPS operating personnel to analyze the event and improve SOL procedures included in the URE electric emergency plan, and provide documentation of the meeting and a copy of the updated electric emergency plan to WECC.
3. Expand the load dispatcher training material related to SOL violations based on what is learned from the analysis of the event, and provide a copy of the expanded load dispatcher training material related to SOL violations to WECC.

URE certified on June 18, 2010 that the above Mitigation Plan requirements were completed on June 1, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE documentation of the meetings with URE BPS operating personnel.
2. Response to the SOL violations plan of the URE electric emergency plan.
3. Updated load dispatcher training material.
4. Documentation of SOL training to URE grid operations load dispatching personnel.

On July 6, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed on June 1, 2010 and that URE was in compliance with TOP-004-2 R1.

TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1

URE's Mitigation Plans to address its violations of TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 were submitted to WECC on April 26, 2010 with a proposed completion date of May 31, 2010. The Mitigation Plans were accepted by WECC on June 9, 2010 and approved by NERC on August 8, 2010. The Mitigation Plans for these violations were submitted as non-public information to FERC on November 17, 2010 in accordance with FERC orders.

Under the Mitigation Plan:

1. URE completed the 2009 ten-year transmission assessment.
2. URE's management and technical staff held discussions and reinforced the importance of issuing the ten-year transmission assessment on a timely basis.

URE certified on May 26, 2010 that the above Mitigation Plan requirements were completed on May 6, 2010. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's 2010 annual progress report.
2. 2009 ten-year transmission assessment that fulfills the milestone activity as submitted in the Mitigation Plan (Section D.3).

On July 9, 2010, after reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plans were completed on May 6, 2010 and that URE was in compliance with TPL-001-0.1 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[26]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[27] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 19, 2011. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a two hundred twenty-five thousand dollar ($225,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE self-reported seven of the violations;
2. URE received only partial self-reporting credit for the CIP-004-1 R2/2.3 violation because the Self-Report was submitted after WECC notified URE that WECC would be conducting a Spot Check;

[26] *See* 18 C.F.R. § 39.7(d)(4).
[27] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC exercised its discretion under Section 3.10 of the NERC Sanction Guidelines and determined the violations of TPL-001-0 R1, TPL-002-0 R1, TPL-003-0 R1 and TPL-004-0 R1 were "related to a single act or common incidence of non-compliance" for which WECC would assess "a single aggregate penalty."
7. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred twenty-five thousand dollars ($225,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as parts of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between WECC and URE entered into as of June 23, 2011, included as Attachment a;

b) Record documents for BAL-004-0 R3:

   1. URE's Self-Report, included as Attachment b-1;
   2. URE's Mitigation Plan designated as MIT-10-2610, included as Attachment b-2;
   3. URE's Certification of Mitigation Plan Completion, included as Attachment b-3;

4. WECC's Verification of Mitigation Plan Completion, included as Attachment b-4;

c) Record documents for CIP-003-1 R1:

1. URE's Source Document, included as Attachment c-1;
2. URE's Mitigation Plan designated as MIT-08-3364, included as Attachment c-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment c-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment c-4;

d) Record documents for CIP-004-1 R2/2.3:

1. URE's Self-Report, included as Attachment d-1;
2. URE's Mitigation Plan designated as MIT-08-2732, included as Attachment d-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment d-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment d-4;

e) Record documents for CIP-004-1 R4:

1. URE's Source Document, included as Attachment e-1;
2. URE's Mitigation Plan designated as MIT-08-3365, included as Attachment e-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment e-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment e-4;

f) Record documents for CIP-007-1 R1 and R2:

1. URE's Self-Certification, included as Attachment f-1;
2. URE's Mitigation Plan designated as MIT-08-2611, included as Attachment f-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment f-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment f-4;

g) Record documents for TOP-004-2 R1:

1. URE's Self-Report, included as Attachment g-1;
2. URE's Mitigation Plan designated as MIT-10-2485, included as Attachment g-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment g-3;

4. WECC's Verification of Mitigation Plan Completion, included as Attachment g-4;

h) Record documents for TPL-001-0.1 R1, included as Attachment h:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as MIT-10-2987, included as Attachment h-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment h-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment h-3;

i) Record documents for TPL-002-0 R1:

1. URE's Self-Report, included as Attachment i-1;
2. URE's Mitigation Plan designated as MIT-10-2988, included as Attachment i-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment i-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment i-4;

j) Record documents for TPL-003-0 R1:

1. URE's Self-Report, included as Attachment j-1;
2. URE's Mitigation Plan designated as MIT-10-2989, included as Attachment j-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment j-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment j-4;

k) Record documents for TPL-004-0 R1:

1. URE's Self-Report, included as Attachment k-1;
2. URE's Mitigation Plan designated as MIT-10-2990, included as Attachment k-2;
3. URE's Certification of Mitigation Plan Completion, included as Attachment k-3;
4. WECC's Verification of Mitigation Plan Completion, included as Attachment k-4;

A Form of Notice Suitable for Publication[28]

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

[28] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001 David N. Cook* Sr. Vice President and General Counsel North American Electric Reliability Corporation 1120 G Street N.W., Suite 990 Washington, DC 20005-3801 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net
Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 213-2673 (801) 582-3918 – facsimile Mark@wecc.biz	Christopher Luras* Manager of Compliance 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
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	*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.

CWhite@wecc.biz Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz	

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001
David N. Cook
Sr. Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, DC 20005-3801
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments