

April 30, 2019

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding [REDACTED],
FERC Docket No. NP19-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty regarding [REDACTED] or The Entity), [REDACTED] [REDACTED] with information and details regarding the nature and resolution of the violation² discussed in detail in the Settlement Agreement attached hereto (Attachment A), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).³

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and The Entity have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violation of CIP-006-3c R2.

According to the Settlement Agreement, The Entity does not contest the violation, but has agreed to actions to mitigate the instant violation and facilitate future compliance under the terms and conditions of the Settlement Agreement.

¹ [REDACTED]
[REDACTED]
[REDACTED]

² 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.

³ See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

NERC Notice of Penalty
The Entity
April 30, 2019
Page 2

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and The Entity. The details of the findings and basis for the [REDACTED] 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 (2018), NERC provides the following summary table identifying the violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violation is set forth in the Settlement Agreement and herein.

* Violation(s) Determined and Discovery Method								
*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation								
NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method*	Violation Start-End Date	Risk	Penalty Amount
WECC2016016712	CIP-006-3c	R2	Medium/Severe	[REDACTED]	SR 12/28/2016	6/1/2016 – 7/1/2017	Serious	No Penalty

WECC2016016712 CIP-006-3c R2- OVERVIEW

The Entity submitted a Self-Report to WECC stating it was in violation of CIP-006-3c R2. The Entity did not document compensating measures to mitigate risk exposure for security patches assessed as applicable but not installed per CIP-007-3a R3, as required by CIP-006-3c R2.

In September of 2016, one of The Entity's Physical Access Control System (PACS) security patch management subject matter experts (SMEs) discovered that some expected security patches had not been deployed to the PACS [REDACTED]. In July 2015, [REDACTED] for the PACS [REDACTED] had reached end-of-life. Sometime in March 2016, security hotfixes were released for the [REDACTED]; however, an incorrect setting on The Entity's [REDACTED], which provides the means to deploy patches, showed that there were no available patches for the Windows Server 2003 during The Entity's April 18, 2016, patch assessment cycle. In May 2016, The Entity identified the previously released [REDACTED] patches, created a package, and presented it to the PACS [REDACTED]. Once presented, the push package installation for the patches failed due to [REDACTED] operability issues. The Entity determined that a manual installation of the patch package would require a reboot of the [REDACTED] however, since the [REDACTED] was at end-of-

NERC Notice of Penalty
The Entity
April 30, 2019
Page 3

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

life and had no backup, rebooting the system may have resulted in system failure. Therefore, The Entity did not install the patch.

The Entity discovered this violation in September 2016, when a PACS SME determined that expected security patches failed to deploy to the [REDACTED]. The Entity did not document compensating measures in place to reduce its risk exposure from not applying applicable security patches. This noncompliance is associated with two PACS [REDACTED], which control physical access to [REDACTED] substations.

The root cause of this violation was less than adequate procedures. Specifically, The Entity's preventive maintenance for equipment did not consider compliance obligations related to end-of-life equipment. Attachment A includes additional facts regarding the violation.

This violation posed a serious risk to the reliability of the bulk power system (BPS). In this instance, The Entity failed to document the compensating measures applied to mitigate the risk where it did not install an applicable patch. Such failure could result in unauthorized access to the vulnerable systems. [REDACTED]

The Entity implemented poor internal controls to reduce the likelihood of harm. The Entity discovered this issue a year after it should have assessed the patches. Moreover, The Entity's ongoing security patch process should have identified the missing security patches during this time. No harm is known to have occurred. Attachment A includes the facts regarding the violation that WECC considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment A and Attachment C include a description of the mitigation activities taken to address this violation. A copy of the Mitigation Plan is included as Attachment C.

The Entity certified that it had completed all mitigation activities. WECC verified that The Entity completed all mitigation activities as of November 15, 2017. Attachments A and D provide specific information on WECC's verification of The Entity's completion of the activities.

Regional Entity's Basis for Penalty

[REDACTED]
[REDACTED]
[REDACTED]

NERC Notice of Penalty
The Entity
April 30, 2019
Page 4

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1. The Entity has previous relevant noncompliance with CIP-006-3c R2 and CIP-007-3c R3. WECC determined The Entity's relevant compliance history with CIP-006-3c R2 to be distinct from the instant noncompliance. WECC considered the RE's relevant compliance history with CIP-007-3c R3 to be an aggravating factor;
2. The Entity had an internal compliance program at the time of the violation. WECC did not apply mitigating credit for the reasons discussed in Attachment A;
3. The Entity self-reported the violation. Nevertheless, WECC did not apply a mitigating credit for self-reporting this violation 210 days after discovery;
4. The Entity was cooperative throughout the enforcement process;
5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. The violation posed a serious or substantial risk to the reliability of the BPS, as discussed in Attachment A; and
7. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the [REDACTED] penalty amount of three hundred fifty-six thousand dollars (\$356,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violation.

NERC Notice of Penalty
The Entity
April 30, 2019
Page 5

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁵

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009, and August 27, 2010 Guidance Orders,⁶ the NERC BOTCC reviewed the violation on November 5, 2018, and approved the resolution between WECC and The Entity. In approving the resolution, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violation at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the [REDACTED] penalty of three hundred fifty-six thousand dollars (\$356,000) is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Request for Confidential Treatment

For the reasons discussed below, NERC is requesting nonpublic treatment of certain portions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publicly, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the Notice of Penalty as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113, respectively.⁷

- a. The Redacted Portions of this Filing Should Be Treated as Nonpublic Under Section 39.7(b)(4) as They Contain Information that Would Jeopardize the Security of the Bulk Power System if Publicly Disclosed

⁵ See 18 C.F.R. § 39.7(d)(4).

⁶ *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

⁷ 18 C.F.R. § 388.113(e)(1).

NERC Notice of Penalty
The Entity
April 30, 2019
Page 6

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Section 39.7(b)(4) of the Commission's regulations states:

The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise.

Consistent with its past practice, NERC is redacting information from this Notice of Penalty according to Section 39.7(b)(4) because it contains information that would jeopardize the security of the BPS if publicly disclosed.⁸ The redacted information includes the identity of the RE, details that could lead to its identification, and information about the security of The Entity's systems and operations, such as specific processes, configurations, or tools the entity uses to manage its cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of The Entity, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."⁹

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of The Entity and any information that could lead to its identification.¹⁰ Information that could lead to the identification of The Entity includes The Entity's name, its NERC Compliance Registry ID, and information regarding the size and characteristics of The Entity's operations.

NERC is also treating as nonpublic any information about the security of The Entity's systems and operations.¹¹ Details about The Entity's systems, including specific configurations or the tools/programs it uses to configure, secure, and manage changes to its BES Cyber Systems, would provide an adversary relevant information that could be used to perpetrate an attack on The Entity and similar entities that use the same systems, products, or vendors.

⁸ NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation. To date, the Commission has directed public disclosure regarding the disposition of CIP violations in only a small number of cases. See Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-019 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). Based on the facts specific to those cases, the Commission directed public disclosure of the identity of the registered entity; the Commission did not disclose other details regarding the CIP violations.

⁹ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204 at P 538 (Order No. 672).

¹⁰ See the next section for a list of this information.

¹¹ See below for a list of this information.

NERC Notice of Penalty
The Entity
April 30, 2019
Page 7

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

- b. The Redacted Portions of this Filing Should Also be Treated as CEII as the Information Could be Useful to a Person Planning an Attack on Critical Electric Infrastructure

In addition to the provisions of Section 39.7(b)(4), the redacted information also separately qualifies for treatment as CEII under Section 388.113 of the Commission's regulations. CEII is defined, in relevant part, as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: (1) relates details about the production, generation, transmission, or distribution of energy; and (2) could be useful to a person planning an attack on critical infrastructure. As discussed above, this filing includes vulnerability and design information that could be useful to a person planning an attack on The Entity's critical infrastructure. The incapacity or destruction of The Entity's systems and assets would negatively affect national security, economic security, and public health and safety. For example, this Notice of Penalty includes the identification of a specific cyber security issue and related vulnerabilities, as well as details concerning the types and configurations of The Entity's systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

In addition to the name of The Entity, the following information has been redacted from this Notice of Penalty:

1. BES Cyber System Information, including security procedures; information related to BES Cyber Assets; individual IP addresses with context; group of IP addresses; Electronic Security Perimeter diagrams that include BES Cyber Asset names, BES Cyber System names, IP addresses, IP address ranges; security information regarding BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, Electronic Access Control and Monitoring Systems that is not publicly available; and network topology diagrams, etc.
2. The names of The Entity's vendors and contractors.
3. The NERC Compliance Registry numbers of The Entity.
4. The registered functions and registration dates of The Entity.
5. The names of The Entity's facilities.
6. The names of The Entity's assets.
7. The names of The Entity's employees.
8. The names of departments that are unique to The Entity.
9. The sizes and scopes of The Entity's operations.
10. The NERC Violation ID of prior instances of noncompliance.

NERC Notice of Penalty
The Entity
April 30, 2019
Page 8

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Under Section 388.113, NERC requests that the CEII designation apply to the redacted information in Items 1-2 for five years from this filing date, April 30, 2019. Details about The Entity's operations, networks, and security should be treated and evaluated separately from its identity to avoid unnecessary disclosure of CEII that could pose a risk to security. NERC requests that the CEII designation apply to the redacted information from Items 3-12 for three years from this filing date, April 30, 2019. NERC requests the CEII designation for three years to allow for several activities that should reduce the risk to the security of the BPS. Those activities include, among others:

1. Compliance monitoring of The Entity to ensure sustainability of the improvements described in this Notice of Penalty; and
2. Remediation of any subsequent violations discovered through compliance monitoring by the Regions.

The Entity should be less vulnerable to attempted attacks following these activities. After three years, disclosure of the identity of The Entity may pose a lesser risk than it would today.

Attachments to be Included as Part of this Notice of Penalty

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

1. Settlement Agreement by and between WECC and The Entity executed October 16, 2018, included as Attachment A;
2. The Entity's Self-Report submitted December 28, 2016, included as Attachment B;
3. The Entity's Mitigation Plan designated as WECCMIT013296 submitted October 13, 2017, included as Attachment C;
4. The Entity's Certification of Mitigation Plan Completion dated December 13, 2017, included as Attachment D; and
5. WECC's Verification of Mitigation Plan Completion issued December 7, 2017, included as Attachment E.

NERC Notice of Penalty
The Entity
April 30, 2019
Page 9

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

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

<p>Melanie Frye*</p> <p>Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6882 (801) 883-6894 – facsimile mfrye@wecc.biz</p> <p>Ruben Arredondo*</p> <p>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</p> <p>Heather Laws*</p> <p>Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz</p> <p>*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.</p>	<p>Edwin G. Kichline*</p> <p>Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net</p> <p>Emily Burgis</p> <p>Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile emily.burgis@nerc.net</p>
---	--

NERC Notice of Penalty
The Entity
April 30, 2019
Page 10

**CONFIDENTIAL AND NON-PUBLIC INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Conclusion

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

Respectfully submitted,

/s/ Emily Burgis

Edwin G. Kichline
Senior Counsel and Director of
Enforcement Oversight
North American Electric Reliability
Corporation

1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

Emily Burgis
Associate Counsel
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
emily.burgis@nerc.net

cc: The Entity
Western Electricity Coordinating Council

Attachments

Attachment A
Settlement Agreement by and between WECC
and [REDACTED] executed October 16, 2018

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

NERC Registration ID: [REDACTED]

Subject: Notice of Revised Expedited Settlement Agreement

[REDACTED],

I. Introduction

The Western Electricity Coordinating Council (WECC) hereby notifies [REDACTED] [REDACTED], that WECC identified Possible Violation of North American Electric Reliability Corporation (NERC) Reliability Standards (Reliability Standards) in the Preliminary Screen process.

WECC has determined that, based on an assessment of the facts and circumstances of the Possible Violation addressed herein, evidence exists that [REDACTED] has an Alleged Violation of the Reliability Standards.

WECC reviewed the Alleged Violation referenced below and determined that this violation is an appropriate violation for disposition through the Expedited Settlement process. In determining whether or not to exercise its discretion to use the Expedited Settlement process, WECC considered all facts and circumstances related to the violation.

This Notice of Expedited Settlement Agreement (Notice) notifies [REDACTED] of the proposed sanction, if any, for such violation. By this Notice, WECC reminds [REDACTED] to retain and preserve all data and records relating to the Alleged Violation.

[REDACTED]

[REDACTED]

II. Alleged Violation

Standard and Requirement	NERC Violation ID	WECC Violation ID
CIP-006-3c R2	WECC2016016712	WECC2016-614264

The attached Expedited Settlement Agreement includes a summary of the facts and evidence supporting each Alleged Violation, as well as other factors affecting disposition determination.

III. Proposed Penalty or Sanction

[REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]²

[REDACTED] compliance history, including this violation, may inform WECC's future monitoring and enforcement strategies. WECC considers the facts and circumstances related to a violation including, but not limited to: 1) Violation Risk Factor; 2) Violation Severity Level; 3) risk to the reliability of the Bulk Electric System (BES)³, including the seriousness of the violation; (4) Violation Time Horizon; 5) the violation's duration; 6) the Registered Entity's compliance history; 7) the Registered Entity's self-reports and voluntary corrective action; 8) the degree and quality of cooperation by the Registered Entity in the audit or investigation process, and in any remedial action; 9) the quality of the Registered Entity's compliance program; 10) any attempt by the Registered Entity to conceal the violation or any related information; 11) whether the violation was intentional; 12) any other relevant information or extenuating circumstances.

IV. Procedures for Registered Entity's Response

If [REDACTED] accepts WECC's proposal that the violation listed in the Agreement be processed through the Expedited Settlement process, [REDACTED] must sign the attached Agreement and submit it through the WECC

¹ 763 F.3d 27 (D.C. Cir. 2014)

² *Id.*

³ "The Commission, the ERO, and the Regional Entities will continue to enforce Reliability Standards for facilities that are included in the Bulk Electric System." (*Revision to Electric Reliability Organization Definition of Bulk Electric System*, 113 FERC ¶ 61,150 at P 100 (Nov. 18, 2010))

Enhanced File Transfer (EFT) Server Enforcement folder within 15 calendar days from the date of this Notice.

If [REDACTED] does not accept WECC's proposal, [REDACTED] must submit a written rejection, through the EFT Server, within 15 calendar days from the date of this Notice, informing WECC of the decision not to accept WECC's proposal.

If [REDACTED] rejects this proposal or does not respond within 15 calendar days, WECC will issue a Notice of Alleged Violation.

V. Disclosure Notice

NERC may include information from this Notice as part of the public record, unless [REDACTED] marks specific information as Confidential Critical Energy Infrastructure Information or Confidential Information in accordance with NERC's Rules of Procedure Section 1500 or the Applicable Governmental Authority's regulations, rules, and orders. It is [REDACTED] responsibility as a Registered Entity to identify any confidential information contained in this Settlement Agreement and to provide supporting justification for designating it as such within five business days after the date of this Notice.

VI. Conclusion

In all correspondence, please provide the name and contact information of a [REDACTED] representative who is authorized to address the above-listed Alleged Violation and who is responsible for providing the required Mitigation Plan. Please also list the relevant NERC Violation Identification Number in any correspondence.

Responses or questions regarding this notice should be directed to Debra Horvath, Senior Enforcement Analyst, at 801-819-7610 or dhorvath@wecc.biz.

Respectfully submitted,



Heather M. Laws

Director, Enforcement

Attachment: Expedited Settlement Agreement

Attachment

EXPEDITED SETTLEMENT AGREEMENT
OF
WESTERN ELECTRICITY COORDINATING COUNCIL
AND
[REDACTED]

Western Electricity Coordinating Council (WECC) and [REDACTED]
(individually a "Party" or collectively the "Parties") agree to the following:

1. [REDACTED] does not contest the violation of the NERC Reliability Standard listed below.
2. The violation addressed herein will be considered a Confirmed Violation as set forth in the NERC Rules of Procedure.
3. [REDACTED] has completed remediation and mitigation activities for the violation listed below.
4. The terms of this Settlement Agreement, including the agreed upon payment, are subject to review and possible revision by NERC and FERC. Upon NERC approval of the Settlement Agreement, NERC will file it with FERC and will post it publicly. If either NERC or FERC rejects the Settlement Agreement, then WECC will attempt to negotiate a revised Settlement Agreement with [REDACTED] that includes any changes to the Settlement Agreement specified by NERC or FERC. If the Parties cannot reach a Settlement Agreement, the CMEP governs the enforcement process.
5. WECC and [REDACTED] have agreed to enter into this Settlement Agreement to avoid extended litigation with respect to the matters described or referred to herein, to avoid uncertainty, and to effectuate a complete and final resolution of the issues set forth herein. WECC and [REDACTED] agree that this Settlement Agreement is in the best interest of the parties and in the best interest of Bulk Power System (BPS) reliability.
6. This Settlement Agreement represents a full and final disposition of the violation listed below, subject to approval or modification by NERC and FERC. [REDACTED] waives its right to further hearings and appeal; unless and only to the extent that [REDACTED] contends that any NERC or FERC action on this Settlement Agreement contains one or more material modifications to this Settlement Agreement.

7. In the event [REDACTED] fails to comply with any of the terms set forth in this Settlement Agreement, WECC may initiate further enforcement actions against [REDACTED] to the maximum extent allowed by federal law and the NERC Rules of Procedure. Except as otherwise specified in this Settlement Agreement, [REDACTED] shall retain all rights to defend against such enforcement actions.
8. This Settlement Agreement shall be governed by and construed under federal law.
9. This Settlement Agreement contains the full and complete understanding of the WECC and [REDACTED] regarding all matters set forth herein. The WECC and [REDACTED] agree that this Agreement reflects all of the terms and conditions of the matters described herein and no other promises, oral or written, have been made that are not reflected in this Agreement.
10. Each of the undersigned warrants that he or she is an authorized representative of the entity designated, is authorized to bind such entity and accepts the Settlement Agreement on the entity's behalf.
11. The undersigned representative of each Party affirms that he or she has read the Settlement Agreement, that all of the matters set forth in the Settlement Agreement are true and correct to the best of his or her knowledge, information and belief, and that he or she understands that the Settlement Agreement is entered into by such Party in express reliance on those representations.
12. This Settlement Agreement and all terms and stipulations set forth herein shall become effective upon FERC's approval of the Agreement by order or operation of law.
13. NOW, THEREFORE, in consideration of the terms set forth herein:

STIPULATED VIOLATION

STANDARD

1. NERC Reliability Standard CIP-006-3c Requirement 2 states:

R2 Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3

Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

VIOLATION FACTS

2. On December 28, 2016, [REDACTED] submitted a Self-Report stating that, as a [REDACTED], [REDACTED] it was in violation of CIP-006-3c R2.
3. Specifically, in September of 2016, one of [REDACTED] Physical Access Control System (PACS) security patch management subject matter experts (SME) discovered that some expected security patches had not been deployed to the [REDACTED] on the PACS [REDACTED]. After researching the issue further, [REDACTED] learned that in July of 2015, the PACS [REDACTED] had reached end-of-life. Sometime in March of 2016, security hotfixes were released for the [REDACTED]; however, an incorrect setting on [REDACTED] [REDACTED] which provides the means to deploy patches, showed that there were no available patches for the [REDACTED] during [REDACTED] April 18, 2016 patch assessment cycle. In May of 2016, [REDACTED] identified the previously released [REDACTED] patches; created a package; and presented it to the PACS [REDACTED]. Once presented, the push package installation for the patches failed due to [REDACTED] operability issues. [REDACTED] determined that a manual installation of the patch package would require a reboot of the [REDACTED]; however; since the device was at end-of-life and had no backup, rebooting the system may have resulted in system failure. Additionally, [REDACTED] did not document compensating measures in place to reduce its risk exposure from not applying applicable security patches. This noncompliance is associated with two PACS [REDACTED] [REDACTED] that control physical access to [REDACTED] substations, which at the time, contained Critical Cyber Assets (CCAs) and now contain Medium Impact Bulk Electric System (BES) Cyber Systems (MIBCS).
4. WECC reviewed the Self-Report and after further discussions with [REDACTED] and analysis of data request responses, determined that [REDACTED] failed to ensure that its PACS were afforded the protective measures required by CIP-006-3c R2, specifically, CIP-007-3c R3, for Security Patch Management.
5. The root cause of this violation was due to less than adequate procedures. Specifically, [REDACTED] preventive maintenance procedures for equipment did not consider compliance obligations related to end-of-live equipment.

6. WECC determined that this violation began on June 1, 2016, when applicable security patches should have been installed or compensating measures to mitigate risk documented and ended on July 1, 2017, when [REDACTED] replaced the two PACS and implemented a CIP Version 5 security patch management program, for a total of 395 days of noncompliance.

RELIABILITY RISK ASESMENT

7. WECC determined that this violation posed a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, [REDACTED] failed to ensure that its PACS were afforded the protective measures specified by CIP-007-3c R3, for Security Patch Management, as required by CIP-006-3c R2.2. Such failure could result in unauthorized access to the vulnerable systems. The unpatched PACS [REDACTED] resided within [REDACTED] corporate networks, [REDACTED]. Unpatched PACS [REDACTED] could potentially allow unauthorized personnel to be granted unescorted physical access to any of the [REDACTED] substations and possibly local electronic access to the associated CCAs, by allowing a malicious actor to hack into the system and make unauthorized changes to the Physical Security Perimeter controls. Unauthorized access due to unpatched software could result in complete control of the unpatched devices due to malware infection or other successful intrusion into the network locations of the unpatched systems. The result could be a complete control (installation of software, exfiltration of data, remote control, etc.) of the affected system and an anchor point for reconnaissance and spreading through the environment, which could have severe negative effects on [REDACTED] connected Cyber Assets and potentially result in significant negative impact to the BES, [REDACTED]

8. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

9. In addition, [REDACTED] implemented poor internal controls. Specifically, [REDACTED] discovered this issue a year after the patches should have been assessed and applied. [REDACTED] on-going security patch management process should have identified the missing security patches during this time, raising concerns about the effectiveness of [REDACTED] entire patch process. [REDACTED]

10. On October 13, 2017, [REDACTED] submitted a Mitigation Plan to address its noncompliance and on December 6, 2017, WECC accepted [REDACTED] Mitigation Plan.

- ### VIOLATION RISK FACTOR (VRF) AND VIOLATION SEVERITY LEVEL (VSL)

- ### OTHER FACTORS AFFECTING DISPOSITION DETERMINATION

16. However, WECC determined that the Expedited Settlement disposition option is appropriate for the following reasons:

- a. The VRF is medium and the VSL is severe for this violation.
- b. WECC determined this violation posed serious and substantial risk to the reliability of the BPS.

- c. WECC considered [REDACTED] CIP-006-3c R2 and CIP-007-3c R3 compliance history in determining the disposition track. [REDACTED] relevant prior noncompliance with CIP-006-3c R2 and CIP-007-3c R3 includes: NERC Violation ID: [REDACTED] [REDACTED], [REDACTED], and [REDACTED].
- i. Regarding [REDACTED] – WECC determined this violation to be an aggravating factor.
 - ii. Regarding [REDACTED] - WECC determined these violations should not be an aggravating factor. The current violation is distinct from these previous violations with this Standard and Requirement. Specifically, [REDACTED] was due to a major delay in receiving hardware; [REDACTED] was due to [REDACTED] not establishing access points; and [REDACTED] was due to poor transition of duties between personnel.
- d. [REDACTED] was cooperative throughout the process. Upon undertaking the actions outlined in the Mitigation Plan, [REDACTED] took voluntary corrective action to remediate this violation. [REDACTED] did not fail to complete any applicable compliance directives. There was no evidence of any attempt by [REDACTED] to conceal the violation. There was no evidence that [REDACTED] violation was intentional. WECC is not aware of any violations of this Reliability Standard by [REDACTED] affiliates or any involvement in [REDACTED] activities such that this violation by [REDACTED] should be treated as recurring conduct.

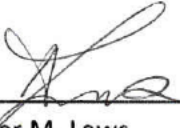
[Remainder of page intentionally left blank - signatures affixed to following page]

Expedited Settlement Agreement

7

Agreed to and Accepted by:

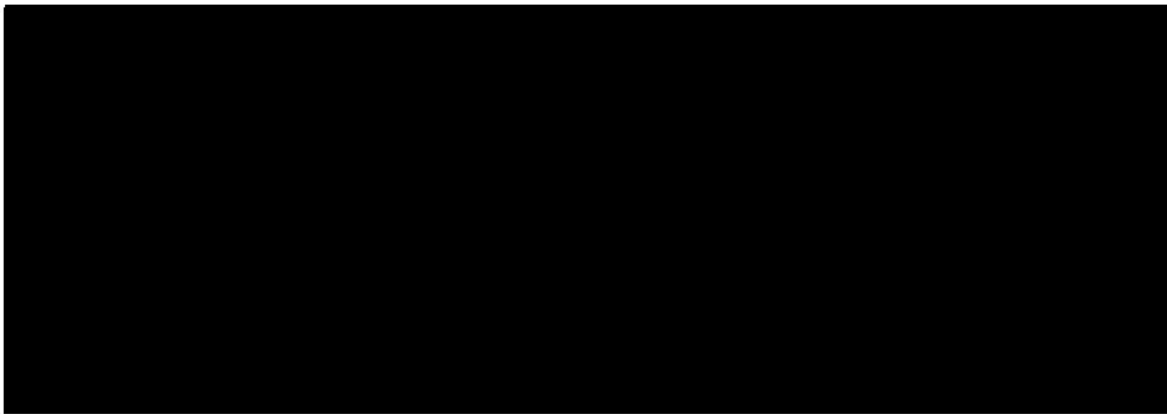
WESTERN ELECTRICITY COORDINATING COUNCIL



Heather M. Laws
Director, Enforcement

10-16-18

Date



Attachment B

Self-Report
submitted December 28, 2016

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-007-6

Requirement: CIP-007-6 R2.

Date Submitted: December 28, 2016

Has this violation previously No
been reported or discovered?:

Entity Information:

Joint Registration
Organization (JRO) ID:

Coordinated Functional
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: August 05, 2016

End/Expected End Date:

Region Initially Determined a June 27, 2016

Violation On:

Reliability Functions: [REDACTED]

Is Possible Violation still Yes
occurring?:

Number of Instances: 3

Has this Possible Violation No
been reported to other
Regions?:

Which Regions:

Date Reported to Regions:

Detailed Description and Control Center
Cause of Possible Violation: In preparation for the CIP V5 audit and resulting WECC data calls, [REDACTED] identified the following significant gaps in evidence to confirm compliance with CIP-007-6 R2:

- R2.1 - The Control Center Source List is not accurate and complete.
 - o Sources are missing because accurate software configuration baseline information is not available for all Cyber Assets.
- R2.2 - Patch Evaluations are not being completed every 35 days.
 - o Consistent enterprise procedures are not implemented in the Control Center for all patch work streams.
 - o Clearer roles and responsibilities have not been established and all responsible personnel are not trained.
- R2.3 - Patch installation or dated mitigation plans are not completed within 35 days following completion of patch evaluations.
 - o Routine installation schedule and procedures are not implemented and/or updated.
 - o Clearer roles and responsibilities are not established and all responsible personnel are not trained.
- R2.4 - Procedures to ensure that mitigation plans are completed within the specified timeframe are not established and administered.

Self Report

underestimated the time required to implement compliance with CIP-007-6 R2. Several elements of the Control Center patch program have yet to be implemented.

was instructed by that their patches and updates for software/firmware provided during the warranty period would be functional rather than security patches and only for proprietary devices. position is that, because the network for the control system is a private network with no external routable connectivity, they do not perform security patching that has the potential to disrupt the operation of the . The network suffered a failure during the trial operation phase due to a setting in a single device being incorrect. position is to not apply security patches for the system devices because they represent a risk to system reliability without providing a tangible security benefit.

has approving authority for implementation of patches for third-party manufactured devices that were utilized by in the system design. Because of this agreement between and the responsibility of evaluating security patches for the third-party devices and Operating System platforms has yet to be defined. After the process for evaluation is determined, an additional process for mitigating the applicable patches during the warranty period will also need to be developed and agreed to between and . The evaluation of security patches for system devices in scope of the requirement and the creation of mitigation plan(s) has not taken place since the requirement became effective on 07/01/16.

PACS

The for the Physical Access Control System (PACS) reached end of life in July 2015. In March 2016, security hotfixes were released for the ; however, an incorrect setting on the , which provides the means to deploy patches, incorrectly showed that there were no available patches for during the 4/18/2016 patch assessment. In May 2016, discovered the patches, created a package, and presented it to the . Once presented, the push package installation for the patches failed due to operability issues. In September 2016, the CIP-007-6 R2 Subject Matter Expert (SME) for PACS discovered that security patches had not been deployed to the server. The cause of this incident was determined to be the result of poor communication between organizations during a transfer of patching responsibilities. There was a misinterpretation of how patches are brought through to the and finally to the server.

cannot install the security hotfixes for the
.
.
.
.

Mitigating Activities:

Description of Mitigating Control Center
Activities and Preventative Compensating measures for the reduction of risk for unpatched systems
Measure: residing within the Control Center apply and are documented as:

1. A network architecture with the most sensitive assets in the innermost layers of the network and firewalls or other access control devices protecting each layer
2. Prohibition of inbound connections into the core of the

Self Report

- [REDACTED] with limited exceptions from Agency-owned networks
- 3. The [REDACTED] provides 24/7 monitoring and alerting capabilities
 - 4. Intrusion detection/protection systems
 - 5. Antivirus tools on all [REDACTED] and [REDACTED] systems
 - 6. Well-defined security configuration standards
 - 7. Centralized log management
 - 8. Centralized testing of security configurations on [REDACTED], [REDACTED] and [REDACTED] operating systems
 - 9. Prohibition of Internet traffic, inbound email and wireless technology

[REDACTED]

[REDACTED] updated the firmware for the [REDACTED] devices during the System Inspection and Repair outage in October 2016. [REDACTED] Cyber Security Manager informed [REDACTED] that [REDACTED] is offering a preliminary patch management service for [REDACTED] starting on or about 11/22/2016. The product will initially be a targeted but untested list of available [REDACTED] patches for [REDACTED] components and non-[REDACTED] third-party vendor provided components. Add-ons to the service will be made available once [REDACTED] North American group has started this initial service. [REDACTED] is now gathering details on the cost and availability of the service.

PACS

After determining that a newer version was available that contained applicable security-related upgrades, the PACS SME updated source documentation to ensure that future patch/firmware reviews are conducted appropriately. All patches to date will be evaluated for applicability. PACS patching will primarily be performed using the [REDACTED]. [REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] is currently upgrading their [REDACTED] system with a new server and upgraded software. The new system is currently being evaluated in the test environment and will be moved to production in January 2017.

Date Mitigating Activities Completed (if applicable): With the exception of the [REDACTED] server, the measures listed in the previous section have already been implemented at [REDACTED]

Have Mitigating Activities No
been Completed?

Date Mitigating Activities
Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: The security updates are relatively low and do not pose an elevated level of risk. There have been no known effects to systems resulting from the vulnerability associated with the patches.

Risk Assessment of Impact to BPS: The layered approach to security at [REDACTED] and the vulnerability addressed by the patches present minimal risk to the BPS.

Additional Entity Comments: N/A

Self Report

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment C

■ Mitigation Plan designated as ■
submitted October 13, 2017

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: [REDACTED]

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
WECC2016016712	CIP-007-6 R2.	12/07/2017

Mitigation Plan Submitted On: October 13, 2017

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: November 15, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On: November 15, 2017

Mitigation Plan Completion Verified by WECC On:

Mitigation Plan Completed? (Yes/No): No

Compliance Notices

Section 6.2 of the NERC CMEP sets forth the information that must be included in a Mitigation Plan. The Mitigation Plan must include:

- (1) The Registered Entity's point of contact for the Mitigation Plan, who shall be a person (i) responsible for filing the Mitigation Plan, (ii) technically knowledgeable regarding the Mitigation Plan, and (iii) authorized and competent to respond to questions regarding the status of the Mitigation Plan. This person may be the Registered Entity's point of contact described in Section B.
- (2) The Alleged or Confirmed Violation(s) of Reliability Standard(s) the Mitigation Plan will correct.
- (3) The cause of the Alleged or Confirmed Violation(s).
- (4) The Registered Entity's action plan to correct the Alleged or Confirmed Violation(s).
- (5) The Registered Entity's action plan to prevent recurrence of the Alleged or Confirmed violation(s).
- (6) The anticipated impact of the Mitigation Plan on the bulk power system reliability and an action plan to mitigate any increased risk to the reliability of the bulk power-system while the Mitigation Plan is being implemented.
- (7) A timetable for completion of the Mitigation Plan including the completion date by which the Mitigation Plan will be fully implemented and the Alleged or Confirmed Violation(s) corrected.
- (8) Implementation milestones no more than three (3) months apart for Mitigation Plans with expected completion dates more than three (3) months from the date of submission. Additional violations could be determined or recommended to the applicable governmental authorities for not completing work associated with accepted milestones.
- (9) Any other information deemed necessary or appropriate.
- (10) The Mitigation Plan shall be signed by an officer, employee, attorney or other authorized representative of the Registered Entity, which if applicable, shall be the person that signed the Self Certification or Self Reporting submittals.
- (11) This submittal form may be used to provide a required Mitigation Plan for review and approval by regional entity(ies) and NERC.

- The Mitigation Plan shall be submitted to the regional entity(ies) and NERC as confidential information in accordance with Section 1500 of the NERC Rules of Procedure.
- This Mitigation Plan form may be used to address one or more related alleged or confirmed violations of one Reliability Standard. A separate mitigation plan is required to address alleged or confirmed violations with respect to each additional Reliability Standard, as applicable.
- If the Mitigation Plan is accepted by regional entity(ies) and approved by NERC, a copy of this Mitigation Plan will be provided to the Federal Energy Regulatory Commission or filed with the applicable governmental authorities for approval in Canada.
- Regional Entity(ies) or NERC may reject Mitigation Plans that they determine to be incomplete or inadequate.
- Remedial action directives also may be issued as necessary to ensure reliability of the bulk power system.
- The user has read and accepts the conditions set forth in these Compliance Notices.

Entity Information

Identify your organization:

Entity Name: [REDACTED]

NERC Compliance Registry ID: [REDACTED]

Address: [REDACTED]

Identify the individual in your organization who will serve as the Contact to the Regional Entity regarding this Mitigation Plan. This person shall be technically knowledgeable regarding this Mitigation Plan and authorized to respond to Regional Entity regarding this Mitigation Plan:

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Violation(s)

This Mitigation Plan is associated with the following violation(s) of the reliability standard listed below:

Violation ID	Date of Violation	Requirement
Requirement Description		
WECC2016016712	08/05/2016	CIP-007-6 R2.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.		

Brief summary including the cause of the violation(s) and mechanism in which it was identified:

The [REDACTED] for the [REDACTED] production Physical Access Control System (PACS) [REDACTED] server reached end of life in July 2015. In March 2016, security hotfixes were released by [REDACTED] for the [REDACTED]; however, [REDACTED] which provides the means to deploy patches, incorrectly showed that there were no available patches for [REDACTED] during the 4/18/2016 patch assessment. In May 2016, [REDACTED] discovered the patches, created a package, and presented it to the [REDACTED]. Once presented, the push package for installation of the patches failed due to [REDACTED] operability issues. In September 2016, the CIP-007-6 R2 Subject Matter Expert (SME) for PACS confirmed that security patches had not been deployed to the [REDACTED] server. The cause of this incident was determined to be the result of poor communication between [REDACTED] organizations during a transfer of patching responsibilities. There was a misinterpretation of how patches are brought through [REDACTED] to the [REDACTED] and finally presented to the [REDACTED]. [REDACTED] has opted not to install the remaining [REDACTED] security hotfixes for the [REDACTED] due to unacceptable risk levels associated with manually rebooting the [REDACTED] considering known stability issues. [REDACTED]

Relevant information regarding the identification of the violation(s):

The mitigation plan for this PNC is to deploy a new PACS system and demonstrate patch compliance on the new system. This work has been completed

Plan Details

Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the violation(s) identified above in Section C.1 of this form:

1. Establish a compliant patch management process for the updated Corporate PACS system.

Provide the timetable for completion of the Mitigation Plan, including the completion date by which the Mitigation Plan will be fully implemented and the violations associated with this Mitigation Plan are corrected:

Proposed Completion date of Mitigation Plan: November 15, 2017

Milestone Activities, with completion dates, that your organization is proposing for this Mitigation Plan:

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
11/15/2017 Milestone	1. Implement Patch Processes for Corp PACS system	11/15/2017	11/15/2017	<p>The PACS system consisting of new [REDACTED] hardware with a supported [REDACTED] and [REDACTED] [REDACTED] was enrolled in a patch management process to maintain compliance with CIP-007-6 R2.</p> <p>[REDACTED] agreed to supply as part of the CMP evidence, an updated system topology diagram for the refreshed PACS system. Additionally, the patch process evidence for June, July and August 2017 will be provided for the refreshed PACS system. The evidence will consist of one patch process document (containing sample evidence of patch evaluation notifications), patching evidence for July, August & September 2017 and a screenshot from the production PACS [REDACTED] showing the current patch level. Patching evidence will contain samples of monthly</p>	No

[Redacted]

December 07, 2017

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending
				evaluation [Redacted] [Redacted] [Redacted] tickets (reoccurring monthly tickets that are closed upon completed evaluation and successful testing), screen-print evidence of applied patches in each environments taken from '[Redacted]' for verification, sample test plans (a part of the monthly testing procedure), and sample e-mail notifications.	

Additional Relevant Information

[Redacted]

Reliability Risk

Reliability Risk

While the Mitigation Plan is being implemented, the reliability of the bulk Power System may remain at higher Risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are known or anticipated : (i) Identify any such risks or impacts, and; (ii) discuss any actions planned or proposed to address these risks or impacts.

The reliability of the HQ PACS is minimally affected until this plan is successfully completed. [REDACTED] currently, and will continue to evaluate [REDACTED] security patches every 35 days. The majority of such patches are deployed within 35 days of evaluation. Only patches which are incompatible or not applicable with applications or databases in our environment are not included. In addition, security patches to major application software, such as [REDACTED], are evaluated every 35 days and are deployed or a mitigation plan is written within 35 days of evaluation. This represents the majority of all potential security patch installations in the environment.

Further compensating measures for the reduction of risk for unpatched systems residing within the PACS operating environments apply and are documented as:

1. A network architecture utilizing [REDACTED]
2. [REDACTED]
3. The [REDACTED] provides 24/7 monitoring and alerting capabilities
4. Antivirus tools on all [REDACTED] systems
5. Well-defined security configuration standards
6. Centralized log management
7. Centralized testing of security configurations on [REDACTED]
8. Prohibition of Internet traffic, inbound email and wireless technology

Prevention

Describe how successful completion of this plan will prevent or minimize the probability further violations of the same or similar reliability standards requirements will occur

In order to reduce risks, the upgraded PACS system employs redundancy of both the PACS [REDACTED] and automated patch deployment tools; for patching, the primary is [REDACTED] and [REDACTED] is the secondary. The PACS applications are hosted in two data-center locations and failed-over during each patching cycle. The PACS [REDACTED] leads a monthly evaluation meeting which includes application, database and infrastructure staff; if found applicable, testing is performed in a separate environment; a security impact analysis is performed and submitted as a part of [REDACTED] prior to deployment into the Production environment. For those patches that are applicable but not deployed, an internal mitigation plan is drafted, and submitted into the monthly [REDACTED] for review by the [REDACTED].

1. [REDACTED]
2. Upon completing the evaluation phase, [REDACTED] is updated to include test results and the risk calculator is attached; a [REDACTED] is issued requesting approval to deploy the patches in the test environment.
3. Upon approval of the [REDACTED], a [REDACTED] is created for [REDACTED] then finally for installation in the [REDACTED]

December 07, 2017

Production environment; the PACS [REDACTED] and PACS System Administrator coordinate the fail-over of the [REDACTED] application server to minimize system interruption to the user community.

Describe any action that may be taken or planned beyond that listed in the mitigation plan, to prevent or minimize the probability of incurring further violations of the same or similar standards requirements

* if applicable, certifies that the Mitigation Plan, as presented, was completed as specified.

1. I am qualified to sign this mitigation plan on behalf of my organization.
2. I have read and understand the obligations to comply with the mitigation plan requirements and ERO remedial action directives as well as ERO documents, including but not limited to, the NERC rules of procedure and the application NERC CMEP.
3. I have read and am familiar with the contents of the foregoing Mitigation Plan.

██████████ Agrees to be bound by, and comply with, this Mitigation Plan, including the timetable completion date, as accepted by the Regional Entity, NERC, and if required, the applicable governmental authority.

Authorized Individual Signature: _____
(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Authorized Individual

Name:

Title: [REDACTED]

Authorized On: October 13, 2017

Attachment D

██████████ Certification of Mitigation Plan Completion
dated December 13, 2017

Certification of Mitigation Plan Completion

Submittal of a Certification of Mitigation Plan Completion shall include data or information sufficient for the Regional Entity to verify completion of the Mitigation Plan. The Regional Entity may request additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6)

Registered Entity Name: [REDACTED]

NERC Registry ID: [REDACTED]

NERC Violation ID(s): WECC2016016712

Mitigated Standard Requirement(s): CIP-007-6 R2.

Scheduled Completion as per Accepted Mitigation Plan: November 15, 2017

Date Mitigation Plan completed: November 15, 2017

WECC Notified of Completion on Date: November 15, 2017

Entity Comment: Please see attached encrypted file "CIP-007-6 R2 P247 CMP [REDACTED].pdf" for mitigation completion evidence.

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	CIP-007-6 R2 P247 CMP [REDACTED].pdf.pgp	Please see attached encrypted file "CIP-007-6 R2 P247 CMP [REDACTED].pdf" for mitigation completion evidence.	12,229,771

I certify that the Mitigation Plan for the above named violation(s) has been completed on the date shown above and that all submitted information is complete and correct to the best of my knowledge.

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature _____ Date _____

(Electronic signature was received by the Regional Office via CDMS. For Electronic Signature Policy see CMEP.)

Attachment E

WECC's Verification of Mitigation Plan

Completion issued December 7, 2017

From: noreply@oati.net
Sent: 12/07/2017 08:18:53

NON-PUBLIC AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED
FROM THIS PUBLIC VERSION

To: [REDACTED]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-6 R2. - [REDACTED]

Please do not REPLY to this message. It was sent from an unattended mailbox and replies are not monitored. If you have a question, send a new message to the OATI Help Desk at support@oati.net.

NERC Registration ID: [REDACTED]
NERC Violation ID: WECC2016016712
Standard/Requirement: CIP-007-6 R2.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [REDACTED] on 11/15/2017 for the violation of CIP-007-6 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

Note: Effective 04/01/2013, WECC will formally notify registered entities of completed Mitigation Plan acceptances via this email notice. WECC will no longer notify entities by uploading a Notice of Completed Mitigation Plan Acceptance letter to the Enhanced File Transfer (EFT) Server.

webCDMS Login: <https://www.cdms.oati.com/CDMS/sys-login.wml>

CONFIDENTIAL INFORMATION: This email and any attachment(s) contain confidential and/or proprietary information of Open Access Technology International, Inc. Do not copy or distribute without the prior written consent of OATI. If you are not a named recipient to the message, please notify the sender immediately and do not retain the message in any form, printed or electronic.

[OATI Information - Email Template: MitPlan_Completed]