NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

August 31, 2020

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. NP20-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding [redacted] and referred to herein as the Entity), NERC Registry ID# [redacted],[2] 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 information and details regarding the nature and resolution of the violations,[4] 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 violations of two serious risk violations, and one moderate risk violation of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards, Order No. 672, 114 FERC ¶ 61,104, order on reh'g, Order No. 672-A, 114 FERC ¶ 61,328 (2006); Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the N. Am. Elec. Reliability Corp., Docket No. RM05-30-000 (February 7, 2008); Mandatory Reliability Standards for the Bulk-Power System, Order No. 693, 118 FERC ¶ 61,218, order on reh'g, Order No. 693-A, 120 FERC ¶ 61,053 (2007).*

[2] The Entity was included on the NERC Compliance Registry as a [redacted]

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

[4] 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.

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

Statement of Findings Underlying the Violations

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 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 (2019), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations 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* & Date	Violation Start-End Date	Risk	Penalty Amount
WECC2017017186	CIP-005-5	R2	Medium/ Moderate	[redacted]	3/1/2017 SR	7/1/2016 – 5/8/2018	Moderate	No Penalty
WECC2017017078	CIP-005-5	R2	Medium/ Moderate	[redacted]	2/22/2017 SR	7/1/2016 – 5/15/2018	Serious	
WECC2017018458	CIP-007-6	R2	High/ Severe	[redacted]	10/5/2017 SR	7/1/2016 – 5/13/2019	Serious	

Background

[redacted]

CIP-005-5 R2

WECC determined that the Entity was not utilizing an Intermediate System (IS) such that Cyber Assets initiating Interactive Remote Access (IRA) did not directly access any Cyber Assets within the Electronic Security Perimeters (ESPs).

The cause of this violation was attributed to the entity's follow up or monitoring of activities not identifying problems. Specifically, the compliance requirements were not clearly understood nor were they validated for completeness.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 1 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 1 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 2.b.

The Entity certified that it had completed all mitigation activities. WECC verified that the Entity had completed all mitigation activities on October 9, 2019. Attachments 1 and 2.d provide specific information on WECC's verification of the Entity's completion of the activities.

CIP-005-5 R2

WECC determined that the Entity did not require multi-factor authentication for all IRA sessions.

The cause of this violation was attributed to the risks or consequences associated with a change not adequately being reviewed or assessed. Specifically, implementation of its multi-factor authentication [redacted] did not take any failure potentials or new provisioning situations into consideration, and no provisions for alternative methods for accomplishing multi-factor authentication were provided.

WECC determined this violation posed a serious and substantial risk to the reliability of the BPS. Attachment 1 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 1 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 3.b.

The Entity certified that it had completed all mitigation activities. WECC verified that the Entity had completed all mitigation activities on September 12, 2019. Attachments 1 and 3.d provide specific information on WECC's verification of the Entity's completion of the activities.

CIP-007-6 R2

WECC determined that the Entity did not (1) have an accurate and complete patch source list; (2) complete patch evaluations every 35 days; (3) within 35 calendar days of the evaluation completion, apply the applicable patches or create a dated mitigation plan; and (4) have procedures established and administered to ensure that mitigation plans were completed within the specified timeframe.

The cause of this violation was attributed to the Entity underestimating the resources and effort required to establish and operate a compliant security patch program under the new requirements for CIP Version 5. Contributing causes included the [redacted]; the complexity of the entity's environment; and the patch program focused on the high impact software to the detriment of the overall program.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS. Attachment 1 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 1 includes a description of the mitigation activities the Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 4.b.

The Entity certified that it had completed all mitigation activities. WECC verified that the Entity had completed all mitigation activities on January 22, 2020. Attachments 1 and 4.d provide specific information on WECC's verification of the Entity's completion of the activities.

Regional Entity's Basis for Resolution of the Violation

According to the Settlement Agreement, WECC has assessed no penalty for the referenced violation. In reaching this determination, WECC considered the following factors:

[redacted]

2. WECC determined the violation of CIP-005-5 R2 Part 2.1 posed a moderate risk and the violations of CIP-005-5 R2 Part 2.3 and CIP-007-6 R2 posed a serious and substantial risk to the reliability of the BPS;
3. The Entity was cooperative throughout the enforcement process;
4. The Entity self-reported all violations in a timely manner from the date of discovery;
5. WECC considered the Entity's prior compliance history with CIP-005-5 R2, and CIP-007-6 R2 to be an aggravating factor.

After consideration of the above factors, WECC determined that it would issue no penalty.

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed[6]

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,[7] the NERC BOTCC reviewed the violation on August 18, 2020 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.

In reaching this determination, the NERC BOTCC considered the factors listed above.

For the foregoing reasons, the NERC BOTCC approved the resolution and believes that the actions are appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[5] [redacted]

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] N. Am. Elec. Reliability Corp., "*Guidance Order on Reliability Notices of Penalty*," 124 FERC ¶ 61,015 (2008); N. Am. Elec. Reliability Corp., "*Further Guidance Order on Reliability Notices of Penalty*," 129 FERC ¶ 61,069 (2009); N. Am. Elec. Reliability Corp., "*Notice of No Further Review and Guidance Order*," 132 FERC ¶ 61,182 (2010).

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.

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 the Entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publically, 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.[8]

a. <u>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</u>

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. NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation.[9] Nonpublic treatment of redacted information, including the identity of the Entity and other details of the violations, depends on: (1) the nature of the CIP violations; (2) whether mitigation is complete; (3) the extent to which the disclosure of the Entity's identity would be useful to someone seeking to cause harm; (4) whether an audit has occurred since the violations; (5) whether the

[8] 18 C.F.R. § 388.113(e)(1).
[9] In response to recent Freedom of Information Act requests, the Commission has directed public disclosure regarding the disposition of CIP violations. See, e.g., Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-19 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). In 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.

violations were administrative or technical in nature; and (6) the length of time that has elapsed since the filing of the Notice of Penalty.[10]

The redacted information in this Notice of Penalty includes details that could lead to identification of the Entity, and information about the security of the Entity's systems and operations, such as specific processes, configurations, or tools the Entity uses to manage their 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."[11]

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.[12] 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.[13] 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.

b. <u>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</u>

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

[10] FOIA No. FY19-30, Second Notice of Intent to Release (June 13, 2019).
[11] *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).
[12] See the next section for a list of this information.
[13] See below for a list of this information.

public health and safety. For example, this Notice of Penalty includes the identification of specific cyber security issues 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 number 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 dates of Compliance Audits of the Entity, as those dates are included in schedules publicly posted by the Regional Entities.
11. The dates of Self-Reports submitted while preparing for Compliance Audits.
12. The Entity's compliance history.

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, August 31, 2020. 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 3-9 for three years from this filing date, August 31, 2020. 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 WECC.

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 March 25, 2020, included as Attachment 1;
2. Record documents for the violation WECC2017017186 of CIP-005-5 R2, included as Attachment 2:
    A. The Entity's Self-Report dated March 1, 2017;
    B. The Entity's Mitigation Plan designated as WECCMIT012868 submitted May 2, 2017;
    C. The Entity's Certification of Mitigation Plan Completion dated May 15, 2018;
    D. WECC's Verification of Mitigation Plan Completion dated October 9, 2019;
3. Record documents for the violation WECC2017017078 of CIP-005-5 R2, included as Attachment 3:
    E. The Entity's Self-Report dated February 22, 2017;
    F. The Entity's Mitigation Plan designated as WECCMIT012790-1 submitted January 25, 2018;
    G. The Entity's Certification of Mitigation Plan Completion dated May 15, 2018;
    H. WECC's Verification of Mitigation Plan Completion dated September 12, 2019;
4. Record documents for the violation WECC2017018458 of CIP-007-6 R2, included as Attachment 4:
    I. The Entity's Self-Report dated October 5, 2017;
    J. The Entity's Mitigation Plan designated as WECCMIT013295-1 submitted May 23, 2018;
    K. The Entity's Certification of Mitigation Plan Completion dated May 13, 2019;
    L. WECC's Verification of Mitigation Plan Completion dated January 22, 2020;

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

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. Melanie Frye President and 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 Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz Heather Laws* 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	Teresina Stasko* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile teresina.stasko@nerc.net James McGrane* Senior Counsel North American Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile james.mcgrane@nerc.net Joshua W. Yang* Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile joshua.yang@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Joshua Yang

Teresina Stasko
Assistant General Counsel and Director of Enforcement
James McGrane
Senior Counsel
Joshua Yang
Associate Counsel
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
teresina.stasko@nerc.net
james.mcgrane@nerc.net
joshua.yang@nerc.net

cc: The Entity
Western Electricity Coordinating Council

Attachments

Attachment 1
Settlement Agreement by and between WECC and [redacted]
executed March 25, 2020

[redacted]

Heather M. Laws
Director, Enforcement
801-819-7642
hlaws@wecc.org

March 2, 2020

Via WECC EFT Server

[redacted]

NERC Registration ID: [redacted]

Subject: Notice of Expedited Settlement Agreement

[redacted]

I. Introduction

The Western Electricity Coordinating Council (WECC) hereby notifies [redacted] ([redacted], that based on an assessment of the facts and circumstances of the Possible Violations addressed herein, evidence exists that [redacted] has Alleged Violations of the Reliability Standards.

WECC reviewed the Alleged Violations referenced below and determined that these violations are appropriate violations for disposition through the Expedited Settlement process. In determining whether to exercise its discretion to use the Expedited Settlement process, WECC considered all facts and circumstances related to the violations.

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

II. Alleged Violations

Standard and Requirement	NERC Violation ID	WECC Violation ID
CIP-005-5 R2	WECC2017017186	WECC2017-614416
CIP-005-5 R2	WECC2017017078	WECC2017-614340
CIP-007-6 R2	WECC2017018458	WECC2017-614663

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][2]

[redacted] compliance history, including these violations, 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 violations listed in the Agreement be processed through the Expedited Settlement process, [redacted] must sign the attached Agreement and submit it through the WECC 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.

[redacted]

[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))

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 includes information from the Settlement Agreement as part of the public record when filed with FERC. It is [redacted] responsibility as a Registered Entity to identify any confidential information contained in the Settlement Agreement, mark said information for redaction (do not apply redaction) as Confidential Critical Energy Infrastructure Information (CEII), and provide to WECC, supporting justification for designating it as such, **within 10 calendar days** after [redacted] execution of the Settlement Agreement.

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 Violations and who is responsible for providing the required Mitigation Plans. Please also list the relevant NERC Violation Identification Numbers in any correspondence.

Responses or questions regarding the Settlement Agreement or for further guidance regarding confidential treatment of CEII should be directed to Debra Horvath, Senior Enforcement Analyst, at 360-823-2453 or dhorvath@wecc.org.

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] ([redacted] (individually a "Party" or collectively the "Parties") agree to the following:

1. [redacted] does not contest the violations of the NERC Reliability Standards listed below.

2. The violations addressed herein will be considered Confirmed Violations as set forth in the NERC Rules of Procedure.

3. [redacted] has completed remediation and mitigation activities for the violations listed below.

4. The terms of this Settlement Agreement 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. The Parties 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. The Parties agree that this Settlement Agreement is in the best interest of each Party and in the best interest of Bulk Power System (BPS) reliability.

6. This Settlement Agreement represents a full and final disposition of the violations 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 Parties regarding all matters set forth herein. The Parties agree that this Settlement Agreement reflects all terms and conditions regarding all matters described herein and no other promises, oral or written, have been made that are not reflected in this Settlement Agreement.

10. Each of the undersigned warrants that he or she is an authorized representative of the Party identified, is authorized to bind such Party and accepts the Settlement Agreement on the Party's behalf.

11. The undersigned representative of each Party affirms that he or she has read the Settlement Agreement, that all 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 Settlement Agreement by order or operation of law.

13. NOW, THEREFORE, in consideration of the terms set forth herein The Parties hereby agree and stipulate to the following:

STIPULATED VIOLATION FACTS

I. NERC RELIABILITY STANDARD CIP-005-5 REQUIREMENT 2

NERC VIOLATION ID: WECC2017017186
WECC VIOLATION ID: WECC2017-614416

STANDARD

1. NERC Reliability Standard CIP-005-5 Requirement 2 states:
   R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.

Part 2.1 Utilize an Intermediate System such hat the Cyber Asset initiating Interactive Remove Access does not directly access an applicable Cyber Asset.

2. On March 1, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-005-5 R2. [redacted]

3. The entity was not utilizing an Intermediate System (IS) such that Cyber Assets initiating Interactive Remote Access (IRA) to [redacted] Electronic Security Perimeters (ESPs) protecting its [redacted], did not directly access any Cyber Assets within the [redacted] ESPs, as required by CIP-005-5 R2 Part 2.1. However, the entity did ensure that electronic remote access to the affected ESPs did require multi-factor authentication. The root cause of this violation was attributed to the entity's follow up or monitoring of activities not identifying problems. Specifically, the compliance requirements were not clearly understood nor were they validated for completeness. This issue began July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on May 8, 2018 when the entity completed mitigating activities, for a duration of 677 days.

RELIABILITY RISK ASSESSMENT

4. WECC determined this violation posed a moderate risk and not a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to utilize an IS such that Cyber Assets initiating IRA to an ESP did not directly access an applicable Cyber Asset within the ESP. as required CIP-005-6 R2 Part 2.1, related to [redacted] of its ESPs.

5. Such failure exposed the Cyber Assets within the ESPs to potential electronic access from external field network laptops and/or corporate computers that could have led to the compromise of said Cyber Assets, which could have in turn resulted in a complete shutdown or unauthorized configuration changes, thereby, affecting any results obtained from the [redacted] itself. Disruption of communications or manipulation of the [redacted] and [redacted] could have led to an inappropriate response by the primary [redacted] controllers and potentially affected the reliability and security of the BPS. Additionally, compromise of network

infrastructure assets contained within the [redacted] could have led to the compromised infrastructure well beyond the scope of these networks, due to common security controls and passwords, which could have significantly impacted the operational Bulk Electric System (BES) across other critical operational networks.

6. However, as compensation, [redacted] Additionally, the [redacted] monitored any failed login attempts and any access into the affected ESPs through any of the EAPs, that included alerts to the [redacted] for any access attempts made during non-business hours. The computers used to electronically access the affected ESPs were patched on a periodic basis and had antivirus and anti-malware software installed.

REMEDIATION AND MITIGATION

7. On May 2, 2017, the entity submitted a Mitigation Plan to address its violation and on December 12, 2017, WECC accepted the entity's Mitigation Plan.

8. To remediate and mitigate this violation, [redacted]
   a. changed electronic access to the [redacted] ESPs in scope to only be allowed through another ESP already utilizing IRA, eliminating the need for separate IRA into the [redacted] ESPs;
   b. determined the ESPs for the Control Centers and identified the new Cyber Assets within the ESPs (four new workstations were added to access field Cyber Assets of the SynchroPhasor-Field system);
   c. updated ESP diagrams to reflect applicable changes;
   d. modified the access control lists (ACLs) for the EAPs to the [redacted] ESPs in scopes so that all electronic access originated from within an ESP already utilizing IRA;
   e. created an architecture that will be utilized for future deployment of [redacted] and other ESP networks;
   f. revised change control and configuration management to access [redacted] devices from within an ESP; and
   g. communicated all changes and revisions to personnel via its shared document repository.

9. On May 15, 2018, the entity submitted a Mitigation Plan Completion Certification and on October 9, 2019, WECC verified the entity's completion of Mitigation Plan.

II. NERC RELIABILITY STANDARD CIP-005-5 REQUIREMENT 2

NERC VIOLATION ID: WECC2017017078
WECC VIOLATION ID: WECC2017-614340

STANDARD

10. NERC Reliability Standard CIP-005-5 Requirement 2 states:

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.

[...]

Part 2.3 Require mult-factor authentication for all Interactive Remote Access sessions.

VIOLATION FACTS

11. On February 22, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance of CIP-005-5 R2. Specifically, due to implementation issues of its [redacted] Card related to users who had lost or damaged their [redacted] Card, the entity resolved to implement an alternative solution for those rare occasions; however, the alternative solution implementation was delayed, so the entity reverted to password only access rather than multi-factor authentication for all IRA sessions as required by CIP-005-5 R2 Part 2.3 at its applicable High and Medium Impact BCSs. Because the entity had not completed the implementation of the alternative solution of a hardware token card program which would allow the local creation and issuance of hardware token smart cards to provide uninterrupted network access to critical applications in the cases where users had a lost or damaged [redacted] Card, there were still occasions when such users were allowed to fall back to password only access until that card could be replaced. Additionally, [redacted] sers who recently had been required by CIP-005-5 R2 to use multifactor authentication to access critical applications did not always use [redacted] Cards to multi-factor authenticate their identities when initiating IRA sessions to High Impact BES Cyber System (HIBCS) IRA access to [redacted] associated with HIBCS located at the Control Center. This issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable and ended on May 15, 2018, when the entity completed mitigating activities to require multi-factor authentication for all IRA sessions at is High and Medium with ERC Impact BCSs, for a violation duration of 684 days.

12. The root cause of the issue was attributed to the risks or consequences associated with a change not adequately being reviewed or assessed. Specifically, implementation of its multi-factor authentication access card system did not take any failure potentials or new provisioning situations into consideration, such as card failures or personnel without access cards. No provision for alternative methods for accomplishing multi-factor authentication were provided. This led to a new group of personnel that did not have access cards, as well as personnel with failed access cards having to use single-factor sign on.

RELIABILITY RISK ASSESSMENT

13. WECC determined this violation posed a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to appropriately implement multi-factor authentication for all IRA sessions, for approximately [redacted] individuals with IRA to [redacted] associated with its HIBCS, as required by CIP-005-5 R2 Part 2.3.

14. Failing to implement multi-factor authentication for IRA sessions could weaken access controls due to the longevity of access passwords and the likelihood of its use on other systems; thereby, creating significant risk that could potentially affect the reliability and stability of the BES, including disruption, manipulation and compromise of communication network systems which could lead to complete control (installation of software, exfiltration of data, remote control, manipulation of data, etc.) of the affected system and an anchor point for reconnaissance and spreading through the environment, which could have severe negative affect on the entity's connected BES Cyber Systems.

15. However, password only access was limited, monitored, and applicable only to individuals that had lost or damaged their [redacted] Cards and a limited number of individuals that did not have access cards. Additionally, Active Directory (AD) was configured to require the use of the multi-factor access card for all remote users, except where they had been explicitly allowed for single-factor access. The AD server was dedicated to the Control Center environment and isolated from the corporate AD environment. Lastly, the entity implemented a process that included the steps used to monitor jumpbox logins while password only authentication was enabled.

REMEDIATION AND MITIGATION

16. On April 4, 2017, the entity submitted a Mitigation Plan to address its violation that WECC rejected on November 13, 2017. The entity resubmitted a Mitigation Plan on January 25, 2018, and on January 29, 2018, WECC accepted the entity's Mitigation Plan.

17. To remediate and mitigate this violation, the entity has:

a. implemented a hardware token program for all IRA sessions that included policies and procedures;
b. developed, tested and published a process to create, issue, revoke, and track hardware tokens;
c. trained all personnel who will utilize hardware tokens;
d. established a contract for professional technical services to include a statement of work defining the expected services;
e. developed, test, and finalized the application installation and AD integration in the lab environment;
f. developed draft system design documents and installation guides;
g. deployed to development environment and gathered required security scans for technology approvals;
h. approved the hardware token technology for the production environment;
i. developed, tested, and finalized the hardware token program in the production environment;
j. created hardware tokens pursuant to the program; and
k. removed any password only access granted to user accounts on the Intermediate Device for HIBCS.

18. On May 15, 2018, the entity submitted a Mitigation Plan Completion Certification and on September 12, 2019, WECC verified the entity's completion of its Mitigation Plan.

III. NERC RELIABILITY STANDARD CIP-007-6 REQUIREMENT 2

NERC VIOLATION ID: WECC2017018458
WECC VIOLATION ID: WECC2017-614663

STANDARD

1. NERC Reliability Standard CIP-007-6 Requirement 2 states:

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.

Part 2.1 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

Part 2.2 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source

or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

Part 2.3 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

Part 2.4 For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

19. On October 5, 2017, the entity submitted a Self-Report stating, as a [redacted] and [redacted] it had a potential noncompliance with CIP-007-6 R2. Specifically, that in preparation for its [redacted] the entity identified significant gaps in evidence to confirm compliance with CIP-007-6 R2 Parts 2.1, 2.2, 2.3, and 2.4 as it relates to the Cyber Assets associated with its [redacted] High Impact BES Cyber System (HIBCS) located at is Control Centers and associated data centers, as well as [redacted] Medium Impact BES Cyber System (MIBCS) with External Routable Connectivity (ERC) located as [redacted] substations. The identified gaps were as follows:

R2.1 - The Control Center Patch Source List was not accurate and complete.

Patch sources were missing because accurate software configuration baseline Information were not available for all applicable Cyber Assets.

R2.2 - Patch Evaluations were not being completed every 35 days.

Consistent enterprise procedures were not implemented in the Control Center for all patch work streams.

Clear roles and responsibilities were not established, and all responsible personnel were not trained in patch evaluation workflow processes and procedures.

R2.3 - Patch installation or dated mitigation plans were not completed within 35 days following completion of patch evaluations.

Routine installation schedule and procedures were not implemented and/or updated.

Clear roles and responsibilities were not established, and all responsible personnel were not trained in patch installation and mitigation plan workflow processes and procedures.

R2.4 - Procedures to ensure that mitigation plans were completed within the specified timeframe were not established and administered.

20. The entity determined that [redacted] Cyber Assets were noncompliant. Specifically, [redacted] in scope included [redacted] (BCAs), 1 [redacted] (EACMS), [redacted] (PACS), and [redacted] (PCAs) associated with [redacted] HIBCS. The remaining [redacted] Cyber Assets included [redacted] BCAs, [redacted] EACMS, and [redacted] PCAs associated with its [redacted] MIBCS. These issues began July 1, 2016 when the Standard and Requirement became mandatory and enforceable and ended on May 13, 2019 when the entity completed mitigation activities, for a duration of 1,047 days of noncompliance. The root cause of this violation was attributed to the entity underestimating the resources and effort required to establish and operate a compliant security patch program for its [redacted] under the new requirements for CIP Version 5. Contributing causes included the lack of a complete inventory of software in the configuration management system; the complexity of the entity's environment; i.e. the volume of various software and device types; and the patch program focused on the highest impact software to the detriment of the overall program.

RELIABILITY RISK ASSESSMENT

21. WECC determined this violation posed a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to effectively implement its process for security patch management [redacted] Cyber Assets related to and associate [redacted] HIBCS and [redacted] related to and associated [redacted] of its MIBCS, for a total [redacted] Cyber Assets [redacted] of the total number of Cyber Assets associated with the aforementioned systems. The failures included identifying a security patch tracking source; evaluating released security patches for applicability within 35 calendar days from the last release; taking action to apply the security patch, creating a mitigation plan, or revising an existing mitigation plan within 35 calendar days of the completion of its evaluation of released security patches, and implementing the mitigation plans within the specified timeframe unless a revision or extension to the mitigation plan is approved by the CIP Senior Manager or delegate, as required by CIP-007-6 R2 Parts 2.1, 2.2, 2.3, and 2.4.

22. Such failures left the Cyber Assets associated with the entity's HIBCS and MIBCS vulnerable. Such vulnerability could have potentially resulted in unauthorized access to the entity's HIBCS and MIBCS. Unauthorized access due to unpatched software could have led to complete control of the affected Cyber Assets due to malware infection or other successful intrusion into the network locations of the unpatched systems. The result could have been a loss of complete control of the affected system and an/or an anchor point for reconnaissance and future spreading of malware through the environment, which could have had severe negative effects on the entity's connected BES Cyber Systems and significant negative affects to the BPS, including potentially

[redacted]

23. However, as compensation the entity had implemented a network architecture with firewalls and other access control devices protecting each network layer. Prohibition of inbound connections into the core of the HIBCS network had limited exceptions from agency-owned networks. The Cyber Assets in scope were monitored and configured for alerting and had antivirus. The entity had implemented intrusion detection and protection systems.

REMEDIATION AND MITIGATION

24. On October 13, 2017, the entity submitted a Mitigation Plan to address its violation and on December 12, 2017 WECC rejected the entity's Mitigation Plan. On May 23, 2018, the entity submitted a revised Mitigation Plan and on June 6, 2018, WECC accepted the entity's Mitigation Plan.

25. To remediate and mitigate the contributing causes of this violation the entity has:
    a. standardized processes and procedures were developed for [redacted] mitigation plans for all Cyber Assets associated with the HIBCS;
    b. consolidated and changed patch source lists to include all software and firmware on the [redacted] for all Cyber Assets associated with the HIBCS and MIBCS located in the Control Center. Indicated on the list all software and firmware that utilize standardized manual patch processes;
    c. trained applicable personnel on manual patch processes and procedures for software and firmware specified on the patch source list as part of the manual patch process for all Cyber Assets associated with the HIBCS and MIBCS located in the Control Center;
    d. implemented standardized Manual Patch Processes for applicable items on the [redacted] for all Cyber Assets associated with the HIBCS and MIBCS located in the Control Center;
    e. standardized [redacted]" and "[redacted]" patch processes and procedures for all Cyber Assets associated with the HIBCS;
    f. revised and updated documentation for "[redacted], and "[redacted]" and included in the [redacted]" workflow for patch discovery through installation for all Cyber Assets associated with the HIBCS and MIBCS located at the Control Center;
    g. merged [redacted]" and [redacted]" patch workflows into the [redacted]" workflow for discovery through installation for all Cyber Assets associated with the HIBCS;

h. included the MIBCS with ERC managed by the Control Center in the [redacted]" and the [redacted]" workflows;
i. identified patch workflows for [redacted]" patch management plan for all Cyber Assets associated with the HIBCS and/or MIBCS.
j. provided Patch Program compliance evidence for systems baselined before December 31, 2017 under CIP-010-2 R1 using the updated Configuration Management System (CMS).
k. developed a process to determine which patches are not applied in [redacted] automatic patch processes and wrote patch mitigation plans where needed;
l. developed a process to identify and communicate security patch information for [redacted] processes and automated [redacted] patch processes that will provide data to be recorded in CMS and reported on baselines;
    i. identification of security vs. not for [redacted] updates to process to attach security info to [redacted] patch signature file;
    ii. developed a function in CMS to read Patch IR tickets for identification of security updates to store in CMS security information for patches and software version updates; and
    iii. developed Security Patch Report in CMS;
m. updated the laptop policy for tools and layered applications to be included in the [redacted] process;
n. produced reports from CMS that identify all [redacted] software titles that are under the Patch Program and the associated workflow [redacted]);
o. conducted a onetime review of installed software versions in the environment in relation to minimum secure version to identify required installations or patch mitigation plans;
p. exercised and proved [redacted] Patch discovery and evaluation process;
q. completed upgrade of [redacted] to a new version in the production environment;
r. developed a process to identify and communicate Windows Security patch information that will be reported from CMS for identification of security vs. not for Windows updates and a process to attach security information to a Windows patch signature file;
s. developed a process to determine which patches are not applied in Windows automatic patch processes and write patch mitigation plans where needed;
t. integrated Patch Source list in CMS to replace tracking spreadsheet;
u. identified all software baselined in CMS that lack current security updates and wrote corresponding patch mitigation plans; and
v. demonstrated one complete patch cycle with full compliance.

26. On May 13, 2019, the entity submitted a Mitigation Plan Completion Certification and on January 22, 2020, WECC verified the entity's completion of Mitigation Plan.

OTHER FACTORS AFFECTING DISPOSITION DETERMINATION

27. [redacted]

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

    a. Base factors:

        i. The Violation Risk Factor for the CIP-005-5 R2 violations is Medium and the Violation Severity Level is Moderate. The Violation Risk Factor the CIP-007-6 R2 violation is High and the Violation Severity Level is Severe.

        ii. WECC determined the CIP-005-5 R2 Part 2.1 posed a Moderate risk and CIP-005-5 R2 Part 2.3 and CIP-007-6 R2 posed a Serious and substantial risk to the reliability of the BPS.

        iii. The three violations have an Operations Planning violation time horizon expectation for remediation of the Requirement from day-ahead up to and including seasonal to preserve the reliability of the BPS.

        iv. The violation duration for CIP-005-5 R2 Part 2.1 was 677 days; for CIP-005-5 R2 part 2.3 it was 684 days, and for CIP-007-6 R2 it was 1,049 as described above.

    b. WECC applied a mitigating factor for the following reasons:

        i. The entity was cooperative throughout the process.

        ii. The entity self-reported both violations in a timely manner from the date of discovery.

    c. WECC applied an aggravating factor for the following reason:

        i. WECC considered the entity's prior compliance history with CIP-005-5 R2 given NERC Violation IDs [redacted] to be relevant and aggravating in consideration of the disposition of the current instant violations.

        ii. WECC considered the entity's relevant compliance history with CIP-007-6 R2 given NERC Violation ID [redacted] to be an aggravating factor.

    d. Other Considerations:

        i. Although the entity has a documented ICP, WECC determined that it was not effective in detecting the violations timely.

        ii. WECC considered the entity's prior compliance history with CIP-005-5 R2 given NERC Violation ID [redacted] to be relevant; however, determined it

[4] [redacted]

should not serve as a basis for aggravating because that violation was of minimal risk and issued in 2011; therefore, not indicative of broader compliance issues.

iii. WECC considered the entity's prior compliance history with CIP-007-6 R2 given NERC Violation ID [redacted] and [redacted] to be relevant; however, determined that these previous violations not serve as a basis for aggravating because 1) [redacted] was discovered and reported during the entity's initial implementation of its CIP-007 security patch management program, whereas the current violation is rooted in the entity's underestimation of resources and effort required to establish and operate a compliant security patch program; and 2) [redacted] was related to a procurement issue and the delay of hardware resulting in the entity moving servers into production without following its prescribed process. As such, the facts, circumstances, and timing of the prior violations are not indicative of a systemic or programmatic issue.

iv. The entity did not fail to complete any applicable compliance directives. There was no evidence of any attempt by the entity to conceal the violation. There was no evidence that these violations were intentional. The entity submitted all requested documentation and/or mitigation plans timely.

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

Agreed to and Accepted by:

WESTERN ELECTRICITY COORDINATING COUNCIL

Heather M. Laws (Mar 25, 2020)

Heather M. Laws
Director, Enforcement

Date

[redacted]

Name:
Title:

Date

Attachment 2.a
[redacted] Self-Report for violation WECC2017017186 of
CIP-005-5 R2 dated March 1, 2017

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-005-5
Requirement: CIP-005-5 R2.
Date Submitted: March 01, 2017
Has this violation previously been reported or discovered?: No

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: March 01, 2017
End/Expected End Date: November 15, 2017
Reliability Functions: [redacted]
Is Possible Violation still occurring?: Yes
Number of Instances: 46
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:
Detailed Description and Cause of Possible Violation: [redacted] does not utilize an Intermediate System on its [redacted] Electronic Security Perimeter (ESP) networks such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

The current method for connecting to the [redacted] requires multi factor authentication but does not occur through use of an intermediate device. The current ESP access point is on a [redacted] that is outside of the site [redacted] ESP.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: [redacted] The [redacted] monitor any failed login attempt and any access into the ESP through any of the access points. Access into the [redacted] ESPs during non-business hours also causes alerts that the [redacted] monitors. The computers used to access the ESP are patched on a periodic basis and

have antivirus and antimalware software that is up to date.

Have Mitigating Activities been Completed? No

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: Degradation of the [redacted] system could have an effect on grid operations and performance.

Risk Assessment of Impact to BPS: The current method to authenticate into the [redacted] ESP and the ability to directly connect to devices can create a potential for exploits. Current access to [redacted] ESPs must originate from the Control Center Network. The current configuration, restricted access and system monitoring are believed to create a low level of risk to [redacted] and the BPS.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 2.b
[redacted] Mitigation Plan designated as WECCMIT012868
submitted May 2, 2017

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: WECCMIT012868

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
WECC2017017186	CIP-005-5 R2.	10/13/2017

Mitigation Plan Submitted On: May 02, 2017

Mitigation Plan Accepted On: December 12, 2017

Mitigation Plan Proposed Completion Date: May 15, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

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		
WECC2017017186	07/01/2016	CIP-005-5 R2.
Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.		

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

[redacted] field sites during our [redacted]. [redacted] does not utilize an Intermediate System on its [redacted] Electronic Security Perimeter (ESP) networks such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. The current method for connecting to the [redacted] requires multi factor authentication but does not occur through use of an intermediate device. The current ESP access point is on a VLAN that is outside of the site [redacted] ESP.

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

The ESP and access controls revision developed under this mitigation plan will not require an intermediate device for accessing the [redacted]) Electronic Security Perimeter (ESP). All access will originate and terminate from within an ESP.

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. Develop a technical solution that only allows access to a site [redacted] ESP from within the [redacted] ESP at another field site or an ESP at a CC. Implement the solution at all [redacted] sites with an ESP and [redacted] CCs. Update documentation for all effected sites and systems.

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: May 15, 2018

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
5/15/2017 Milestone	1. Develop a project plan to change access to the [redacted] ESP at field sites to only be from another ESP. 2. Develop draft ESP diagrams for field sites to depict the proposed change.	05/15/2017	05/15/2017	1. A project plan to change access to the [redacted] ESP at field sites to only be from another ESP was created.. 2. Draft ESP diagrams are created for field sites to depict the proposed change.	No
8/15/2017 Milestone	3. Determine the ESP for the control centers. Identify the new Cyber Assets within the ESP(s). 4. Update ESP Plans if needed [redacted] 5. Develop modified access control lists for the routers at [redacted] field sites so that all access originates from within an ESP. 6. Test and verify the Access Control Lists	08/15/2017	08/15/2017	3. The [redacted] control center ESPs will be used for the [redacted] control center to access field cyber assets of the SynchroPhasor system. 4. The ESP plan has been updated to document the new subnet that will be added to the [redacted] ESP's. The ESP diagram was also amended to show the new subnet. These documents will be "published" once the project is complete.	No

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
	(ACL) and approve for deployment to the sites with the [redacted] Field BES cyber system. 7. Develop a schedule for the deployment to the [redacted] field sites.			5. The existing inbound ACLs at [redacted] field sites will be used in conjunction with [redacted] Secure Access Control System (ACS) and an additional outbound ACL to provide the necessary access restriction to make sure the VPN origin is from another ESP. 6. A test plan was developed and deployed in the test environment. Tests were conducted to confirm access was limited to ESP to ESP with denial for all other VPN origins. 7. A schedule has been developed to deploy the technical solution to all [redacted] field sites.	
11/15/2017 Milestone	8. Deploy the ACLs to 15 [redacted] Sites. 9. Update and publish the ESP diagram [redacted]	11/15/2017	11/15/2017	8[redacted] 9. The changes implemented on the listed sites conform to the	No

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
				Standard Substation ESP diagram for [redacted] sites.	
2/15/2018 Milestone	10. Deploy the ACLs to [redacted] Sites. 11. Update and publish the ESP diagram [redacted]	02/15/2018			No
5/15/2018 Milestone	12. Deploy the ACLs to the remaining [redacted] Sites. 13. Update and publish the ESP diagram.	05/15/2018			No

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.

To gain interactive remote connectivity to the BES asset within the [redacted] monitor any failed login attempts and any access into the ESP through any of the access points. Access into the [redacted] ESPs during non-business hours also causes alerts that the [redacted] monitors. The computers used to access the ESP are patched on a on-going basis and have antivirus and antimalware software that is up to date.

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

The only allowed access to the [redacted] ESP will be from another ESP. This will not require that an intermediate device is used to gain access.

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

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

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

Acknowledges:

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.

[redacted] 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: [redacted]

Title: [redacted]

Authorized On: May 02, 2017

Attachment 2.c
[redacted] Certification of Mitigation Plan Completion for
violation WECC2017017186 of CIP-005-5 R2
dated May 15, 2018

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): WECC2017017186

Mitigated Standard Requirement(s): CIP-005-5 R2.

Scheduled Completion as per Accepted Mitigation Plan: May 15, 2018

Date Mitigation Plan completed: May 15, 2018

WECC Notified of Completion on Date: May 15, 2018

Entity Comment: Please see attached encrypted file [redacted]

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	Please see attached encrypted file [redacted] for [redacted] evidence of completion	5,137,521

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 2.d
WECC's Verification of Mitigation Plan Completion for violation
WECC2017017186 of CIP-005-5 R2 dated October 9, 2019

From: noreply@oati.net
Sent:
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-005-5 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 I[redacted]
NERC Violation ID: WECC2017017186
Standard/Requirement: CIP-005-5 R2.
Subject: Completed Mitigation Plan Acceptance

WECC received the Certification of Mitigation Plan Completion submitted by [redacted]on 05/15/2018 for the violation of CIP-005-5 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 3.a
[redacted] Self-Report for violation WECC2017017078 of CIP-005-5 R2
dated February 22, 2017

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-005-5
Requirement: CIP-005-5 R2.
Date Submitted: February 22, 2017
Has this violation previously been reported or discovered?: No

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: November 18, 2016
End/Expected End Date: November 15, 2017
Reliability Functions: [redacted]
Is Possible Violation still occurring?: Yes
Number of Instances: 1
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [redacted] has implemented the [redacted] Card in compliance with [redacted] which also meets compliance with CIP-005-5 R2.3. With the implementation of the [redacted] card, [redacted] has met with problems introduced by users who have lost or damaged their card. The project to implement an alternate solution for these rare occasions have not been completed and the current resolution is to use password only access.

Because [redacted] has not completed the implementation of the planned hardware token card program which will allow the local creation and issuance of hardware token smart cards which can provide uninterrupted network access to critical applications in the case where users have a lost or damaged [redacted] Card, there are still occasions when such users must be allowed to fall back to password only access until that card can be replaced.

Additionally, [redacted] users who recently have been required to cross the CIP boundary to access critical application do not yet use [redacted] cards to multi-factor authenticate their identities when crossing electronic security perimeter (ESP) boundaries to access High BES systems. [redacted] schedulers in their control room do not have [redacted] readers available on all machines and have not had time to test their 24/7 functional capability once [redacted] cards are fully enforced.

Until both of these issues are resolved, [redacted] Control Centers will not be fully capable of enforcing 100% multifactor authentication for all remote application

users connecting across the ESP boundary.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Access to the BES systems still requires single factor authentication. Password only access is limited, monitored and applicable only to individuals that have lost or damaged their [redacted] card.

Have Mitigating Activities been Completed? No

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: Inappropriate access to High BES systems could have significant effects on the reliability and stability of the BES. To date there have been no instances of inappropriate use resulting from the access of BES systems through single factor authentication.

Risk Assessment of Impact to BPS: Since the use of single factor authentication for electronic access is intermittent in nature and two-factor authentication is required for physical access to the work area, there is minimal risk to the BES.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 3.b
[redacted] Mitigation Plan designated as WECCMIT012790-1
submitted January 25, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017017078	CIP-005-5 R2.	10/13/2017

Mitigation Plan Submitted On: January 25, 2018

Mitigation Plan Accepted On:

Mitigation Plan Proposed Completion Date: May 15, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

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		
WECC2017017078	07/01/2016	CIP-005-5 R2.
Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.		

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

[redacted] users were not using multi-factor [redacted] cards) authentication to gain access from outside the electronic security perimeter (ESP) to BES Cyber Systems in the ESP. [redacted] in their control room, which is outside of the ESP, do not currently have [redacted] readers available on all machines to enforce multi-factor authentication, Additionally users attempting to gain access to BES Cyber Systems from outside the ESP may lose, misplace or forget their [redacted] cards from time to time that would require the Intermediate Device (Jump-host) to be configured to allow username and password authentication in order to sustain business functions and services.

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

The program developed under this mitigation plan will enforce the multifactor authentication requirement (CIP 005-5 R2.3)to access from outside the ESP to BES Cyber Systems within the Control Center ESP and PSP.

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. Develop a Control Center Hardware token program that only allows Control Center support staff to issue individuals an additiona[redacted] card to [redacted] personnel requiring Interactive Remote Access (IRA) to BES Cyber Systems within the ESP. The additional [redacted] card will enforce multi-factor authentication for all [redacted] personnel requiring IRA to Control Center BES Cyber Systems.

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: May 15, 2018

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
1/26/2018 Milestone	1. Implement interim process to monitor jumpbox logins when password "only" authentication is enabled 2. Publish [redacted] 3. Develop, test and publish process to create, revoke, issue and track [redacted] 4. Contract in place for Professional Technical Services	01/26/2018	01/25/2018	1. An interim process and monitoring controls have been implemented. See attached file [redacted] 2. [redacted] was approved and published to the Control Center Library. 3. A single procedure to create, revoke, issue, track and retrieve [redacted] has been developed 4. The contract for professional services was put in place with a Statement of Work defining the expected services.	No
2/15/2018 Milestone	5. Develop, test and finalize the application installation and AD integration in the [redacted] environment. 6. Develop draft	02/15/2018			No

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
	system design documents and installation guides.				
5/15/2018 Milestone	7. Deploy to DEV environment and gather required security scans for technology approvals 8. Approve the [redacted] technology for the production environment [redacted]. 9. Develop, test and finalize the [redacted] program in the production environment. 10. Issue cards to applicable users in [redacted]. 11. Remove any password only access granted to user accounts on the Intermediate Device for CC systems	05/15/2018			No

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 risk to the reliability of the BPS remains low until this mitigation plan is implemented. The network security architecture is based on a defense in depth strategy that includes, dedicated point-to-point firewalls, Intrusion Detection Systems and Intrusion Prevention Systems. User authentication to the BES Cyber System is through a controlled Intermediate Device. Furthermore, the physical location of the workstations used to access the BES Cyber Systems is in a controlled room within a corporate building. Physical access to the corporate building and controlled room both require a badge to gain access.

Remediation Activities: The use of password only user access will be controlled by [redacted] This document explains how to activate and terminate the settings on the jump box and describes the monitoring controls implemented to minimize the increased risk associated with password only authentication. [redacted] all other intermediate devices used for access retain multifactor authentication. The [redacted] will monitor and respond to alerts according to '[redacted] This interim process does not allow users open access to the control center network or systems from the intermediate device, Active Directory manages individual user permissions to the BCSs and access to the BCSs is through the jump box. All access to intermediate devices originates from the [redacted] within secure [redacted] facilities

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

The adoption of the [redacted] will require that all users requiring IRA to Control Center BES Cyber Systems will be required to either use their [redacted] card or their [redacted] for multi-factor authentication.. Both the [redacted] card and [redacted] will only authorize IRA users into the ESP environment. Application level authentication and authorization will be addressed by appropriate groups once the [redacted] program is complete. Access using password only for authentication will not be permitted for interactive and/or remote desktop services logon.

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

The deployment of additional systems such as [redacted] along with application level changes will likely be required to support [redacted] card or [redacted] logon for applications that require authentication.

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

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

Acknowledges:

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.

[redacted] 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: [redacted]

Title: [redacted]

Authorized On: January 25, 2018

Attachment 3.c
[redacted] Certification of Mitigation Plan Completion for violation
WECC2017017078 of CIP-005-5 R2 dated May 15, 2018

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): WECC2017017078
Mitigated Standard Requirement(s): CIP-005-5 R2.
Scheduled Completion as per Accepted Mitigation Plan: May 15, 2018
Date Mitigation Plan completed: May 15, 2018
WECC Notified of Completion on Date: May 15, 2018
Entity Comment: Please see attached encrypted file [redacted] for [redacted] evidence of completion

Additional Comments		
From	Comment	User Name
Entity	Interim process and monitoring controls have been implemented. See attached data request [redacted]	Christine Jensen

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	Remediation activities are described in the document [redacted] This document is attached to the data request [redacted]	225,958
Entity	[redacted]	Please see attached encrypted file [redacted] completion	32,529,380

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 3.d
WECC's Verification of Completion of Mitigation Plan for
violation WECC2017017078 of CIP-005-5 R2
dated September 12, 2019

From: noreply@oati.net
Sent: 10/09/2019 11:07:23
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-005-5 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: WECC2017017078
Standard/Requirement: CIP-005-5 R2.
Subject: Completed Mitigation Plan Acceptance

WECC received the Certification of Mitigation Plan Completion submitted by [redacted] on 05/15/2018 for the violation of CIP-005-5 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 4.a
[redacted] Self-Report for violation of CIP-007-6 R2
dated October 5, 2017

Self Report

Entity Name: [redacted]
NERC ID: [redacted]
Standard: CIP-007-6
Requirement: CIP-007-6 R2.
Date Submitted: October 05, 2017
Has this violation previously been reported or discovered?: No

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: July 01, 2016
End/Expected End Date: October 15, 2018
Reliability Functions: [redacted]
Is Possible Violation still occurring?: Yes
Number of Instances: 216
Has this Possible Violation been reported to other Regions?: No
Which Regions:
Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [redacted], [redacted] identified the following significant gaps in evidence to confirm compliance with CIP-007-6 R2:

[redacted] R2.1 - The Control Center Source List is not accurate and complete.
• Sources are missing because accurate software configuration baseline Information is not available for all Cyber Assets.

[redacted] R2.2 - Patch Evaluations are not being completed every 35 days.
• Consistent enterprise procedures are not implemented in the Control Center for all patch work streams.
• Clearer roles and responsibilities have not been established and all responsible personnel are not trained.

[redacted] R2.3 - Patch installation or dated mitigation plans are not completed within 35 days following completion of patch evaluations.
• Routine installation schedule and procedures are not implemented and/or updated.
• Clearer roles and responsibilities are not established and all responsible personnel are not trained.

[redacted] R2.4 - Procedures to ensure that mitigation plans are completed within the specified timeframe are not established and administered.

The root cause is a lack of resources applied to fully develop and implement a compliant patch program. [redacted] underestimated the difficulty and time required to implement a robust patch management program in conjunction with a configuration management system and associated processes and procedures.

Self Report

Contributing causes included the lack of a complete inventory (Asset Baselines CIP-010-2 R1) of software and firmware in the configuration management system including installed patches; the complexity of [redacted] environment i.e. the sheer number of different software and device types. The patch program focused on the highest impact software, [redacted] to the detriment of the overall program.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Compensating measures for the reduction of risk for unpatched systems residing within the Control Center apply and are documented as:
1. Security patches and updates for [redacted] operating systems are being discovered, evaluated, and applied on a 35 day cycle for network connected devices. [redacted] available security patches and updates affecting the BES Cyber Systems in the Control Centers.
2. 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
3. Prohibition of inbound connections into the core of the Control Center [redacted] with limited exceptions from [redacted]
4. The Control Center [redacted] provides 24/7 monitoring and alerting capabilities
5. Intrusion detection/protection systems
6. Antivirus tools on all [redacted] systems
7. Well-defined security configuration standards
8. Centralized log management
9. Centralized testing of security configurations on [redacted] operating systems
10. Prohibition of Internet traffic, inbound email and wireless technology

Have Mitigating Activities been Completed? No

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: Security updates are being installed in the CC environment. The current processes require extensive manual intervention to determine what patches are applied to cyber assets. The work is being done but the documentation is cumbersome. There have been no known effects to systems resulting from vulnerabilities associated with the patches.

Risk Assessment of Impact to BPS: The layered approach to security at [redacted] working in tandem with monitoring make the vulnerabilities addressed by the patches present a minimal risk to the BPS.

Additional Entity Comments: [redacted]

Self Report

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 4.b
[redacted] Mitigation Plan designated as WECCMIT013295-1
submitted May 23, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: WECCMIT013295-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017018458	CIP-007-6 R2.	12/08/2017

Mitigation Plan Submitted On: May 23, 2018

Mitigation Plan Accepted On: June 01, 2018

Mitigation Plan Proposed Completion Date: May 15, 2019

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [redacted] On:

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		
WECC2017018458	07/01/2016	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:

[redacted] evaluated the CC patch program and identified gaps in evidence to confirm compliance with CIP-007-6 R2 for High BES cyber assets and Medium BES cyber assets under CC management:
• R2.1 - The Control Center Source List used for patch discovery was not accurate and complete. 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 Clear 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 the completion of security patch evaluations and applicability is determined.
o Routine installation schedule and procedures are not implemented and/or updated for all patch work streams.
o Clear 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.

[redacted] underestimated the time and complexity required to implement compliance with CIP-007-6 R2.

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

[redacted], [redacted] identified significant gaps in evidence to confirm compliance with CIP-007-6 R2. The effort to patch CC devices is significant but the current processes do not produce evidence to confirm compliance.

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. [redacted] will implement a new project to ensure Control Center Security Patch Management Program is sustainable and meets compliance requirements for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCAs, and Medium Impact BES Cyber Systems maintained by the CC and their EACMS and PCAs. Patch processes for PACS for Medium Impact BES cyber systems is under a separate organization that is not part of the CC processes.
2. [redacted] will evaluate all automated and manual patch processes and procedures and make modifications as necessary to implement an updated Control Center Security Patch Management Program to ensure:
a. Control Center Patch Source List is maintained accurately to reflect installed software and firmware for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained be the CC and their EACMS and PCA.
b. Security Patch Evaluations are completed every 35 days for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained be the CC and their EACMS and PCA.
c. Security Patch installation or dated mitigation plans are completed within 35 days for applicable security patches for all for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained by the CC and their EACMS and PCA.
3. [redacted] will develop and/or update patch installation processes designed to install security patches for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained be the CC and their EACMS and PCA.
4. [redacted] will develop a Mitigation Plan management process that ensures security patch mitigation plans are actively managed to ensure they are completed within the established specified timeframe; or revised and approved by the NERC CIP Senior Manager for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained by the CC and their EACMS and PCA.
5. [redacted] will provide staff training on the updated Security Patch processes for all High Impact BES Cyber Systems and their associated EACMS, PACS and PCA and Medium Impact BES Cyber Systems maintained be the CC and their EACMS and PCA.

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: May 15, 2019

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. Develop standardized processes and procedures for "Manual Patch" Discovery, Assessment, and Patch mitigation	11/15/2017	11/15/2017	The project has been working on maturing the Control Center (CC) patch program and closing the gaps identified in the processes and procedures in order to achieve and sustain compliance with	No

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
	plans applicable to Control Center (CC) BCAs. 2. Consolidate patch source lists and include all software and firmware on the [redacted] for all CC BCAs. Indicate on the list all software and firmware that utilize standardized manual patch processes. 3. Train personnel on manual patch processes and procedures for identified software and firmware specified on the patch source list as part of the manual patch process applicable to CC BCAs. 4. Implement standardized Manual Patch Processes for applicable items on the Manual Patch Source list for CC BCAs. 5. Update standardized [redacted] and [redacted] patch processes and procedures applicable to CC BCAs. 6. Complete documentation for			CIP-007-6 R2 and all sub-requirements (R2.1-R2.4). Activities completed for this quarterly milestone update that align with the project deliverables are as follows: 1. Standardized processes and procedures were developed for "Manual Patch" Discovery, Assessment, and Patch mitigation plans applicable to CC BCAs. The processes are: • [redacted] • [redacted] • [redacted] • [redacted] 2. Patch source lists were consolidated and changed to include all software and firmware on the [redacted] for all CC BCAs. The patch source list indicates on the list all software and firmware that utilize standardized manual patch processes. The patch source list is: • [redacted] 3. Applicable personnel were	

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
	[redacted] and [redacted] patch work flows for patch discovery through installation for the CC.			trained on manual patch processes and procedures for software and firmware specified on the patch source list as part of the manual patch process applicable to CC BCAs. The training material and rosters are listed below. • [redacted] • [redacted] 4. Standardized Manual Patch Processes for applicable items on the Manual Patch Source list for CC BCAs are implemented. The standardized process are: • [redacted] • [redacted] • [redacted] 5. Standardized [redacted] and [redacted] patch processes and procedures applicable to CC BCAs. Have been updated to conform to CIP-007-6 R2. Applicable processes are: • [redacted] • [redacted]	

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
				[redacted] • [redacted] • [redacted] An example [redacted] ticket to be provided. • [redacted] 6. Documentation for [redacted] and [redacted] patch work flows for patch discovery through installation for the CC has been revised and updated. Applicable processes are: • [redacted] • [redacted] • [redacted] • [redacted]	
2/15/2018 Milestone	7. Complete documentation for [redacted] and [redacted] patch work flows for patch discovery through installation applicable to CC BCAs. 8. Complete documentation for the CC "BES Medium	02/15/2018	02/15/2018	7). Manual with Periodic Installation The Manual with Periodic Installation workflow was determined to be the same as the standard Manual Patch workflow with the addition of an accumulating patch mitigation plan that is scheduled for the next scheduled maintenance. This covers devices that are only updated on a	No

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
	Impact" patch program. This covers the [redacted] documentation for [redacted] patch management plan for the control center. 10. Provide Patch Program compliance evidence for systems baselined before 12/31/2017 under CIP-010-2 R1 using the updated [redacted]			maintenance interval that exceeds 35 days. 7). [redacted] workflow is also included in the Manual Patch workflow; Discovery is performed manually and Assessment is performed by manual review of the patches that are installed on the [redacted] The schedule for network connected devices will follow the automated monthly patch schedule. [redacted] fall under the Manual or Manual with Periodic Installation workflows. 8) BES Medium Impact w ERC managed by Control Center The proposed BES Medium Impact workflow has been included in the Manual Patch Workflow and the [redacted] and Switch Patch Workflow. The work to get all of the patch sources for [redacted] is still in progress. 9) Transient Cyber Assets Transient Cyber Assets, TCA, in the Control Centers consist of laptop computers that are managed following the Laptop and Portable Computer Policy - Standards. These standards require that each TCA have a home network outside of the ESP that	

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
				provides automated [redacted] patching. All other software is patched using the manual patch process. Work to identify all installed software will be included on the Patch Source List. 10) The patch program compliance evaluation for [redacted] was completed. The results are shown on a spreadsheet for each system. The spreadsheet identifies all of the installed technology versions and the relationship to the patch source list. This work was completed to ensure that all technologies were enrolled in a patch workflow.	
5/15/2018 Milestone	11. Provide Patch Program compliance evidence for the remaining systems baselined under CIP-010-2 R1 using the updated Configuration Management System.	05/15/2018	05/15/2018	Modifications completed in [redacted] tickets that are used to document evaluation and applicability of security patches Developed process for identification of [redacted] signatures reported to [redacted] for baseline updates resulting from automatic patch process applied with [redacted] and [redacted]. This work is still under development to provide the required reliability in baseline updates. Completed security test plan for pre-production security controls evaluation using the automated patch	No

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
				test servers. For the period from November 2017 - May 2018 there have been manual patch discoveries for[redacted] software titles resulting in [redacted] evaluation tickets, [redacted] planning tickets and [redacted] patch mitigation plan tickets For the most recent automated patch cycle. • [redacted] o [redacted] o [redacted] o [redacted] o [redacted] • [redacted] o [redacted] o [redacted] Issue Summary: Incomplete [redacted] baseline data and the lack of a suitable report required the Patch Program to attempt to use raw [redacted] data to identify the software in the environment and determine the gap between the current installed versions and their minimum secure version. This manual process was too complex, time consuming and unreliable. Sustained compliance for the Patch Program could not be built on this method.. Some aspects of automated	

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
				patch processes have just become operational and are not fully integrated with [redacted] and require additional time to identify and fix process weaknesses between patching and updating [redacted] baselines accurately and within the 30 day period. The Patch Program has not established a process for identification of security (as opposed to all) updates and patches. Security patch identification and determination of patches not installed remain as gaps to achieve compliance for CIP-007 and CIP 010. Automated patch processes for [redacted] environments have been occurring every 35 days but the tool is currently broken for a second time this year. The existing version of [redacted] has recently gone out of support and updates from the vendor have caused [redacted] to operate incorrectly and pose a risk to reliable operations of BCS.	
8/15/2018 Milestone	1. Develop a process to determine which patches are not applied in [redacted] automatic patch processes and write patch mitigation plans where needed.	08/15/2018			No

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
	2. Develop a process to identify and communicate Security patch information for manual patch processes and automated[redacted] patch processes that will provide data to be recorded in [redacted] and reported on baselines. o Identification of security vs. not for [redacted] updates o Process to attach security info to[redacted] patch signature file o Function in [redacted] to read [redacted] tickets for identification of security updates o Storage in [redacted] of security info for patches and software version updates o Develop Security Patch Report in [redacted] 3. Update the laptop policy for tools and layered applications to be included in the manual patch process.				
11/15/2018 Milestone	4. Produce reports from [redacted] that identify all [redacted] software titles that are under the Patch Program and the associated workflow (manual or automated). 5. Process to	11/15/2018			No

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
	evaluate installed software versions in the environment in relation to minimum secure version to identify required installations or patch mitigation plans. 6. Exercise and prove [redacted] Patch discovery and evaluation process.				
2/15/2019 Milestone	7. Complete upgrade [redacted] to new version in Production environment 8. Develop a process to identify and communicate [redacted] patch information that will be reported from [redacted] o Identification of security vs. not for [redacted] updates o Process to attach security info to [redacted] patch signature file 9. Develop a process to determine which patches are not applied in [redacted] automatic patch processes and write patch mitigation plans where needed. 10. Integrate Patch Source list in [redacted] replacing spreadsheet. 11. Identify all software baselined in [redacted] that lack current security updates and write	02/15/2019			No

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
	corresponding patch mitigation plans.				
5/15/2019 Milestone	12. Demonstrate one complete patch cycle with full compliance by May 15, 2019	05/15/2019			No

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 BES 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 automatically deployed [redacted] within 35 days of evaluation. Only patches which are incompatible with applications in our environment are not included. In addition, security patches to major application software, such as EMS, 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. This mitigation is to establish a program to ensure the discovery and assessments are timely, patch mitigations are tracked and the patch versions on any applicable device for installed software/firmware is known.

Further compensating measures for the reduction of risk for unpatched systems 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 [redacted] with limited exceptions from [redacted]
3. The [redacted] provides 24/7 monitoring and alerting capabilities
4. Intrusion detection/protection systems
5. Antivirus tools on all [redacted] systems
6. Well-defined security configuration standards
7. Centralized log management
8. Centralized testing of security configurations on [redacted] operating systems

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

Successful completion of this plan will provide clear and consistent processes, procedures, and roles for patching including discovery, evaluation, installation, mitigation plans, and verification. The plan provides for tracking mitigation plans and patch installations. All known software will be included in one patch source list which will also identify the associated patching workflow and the responsible staff.

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

Authorization

An authorized individual must sign and date the signature page. By doing so, this individual, on behalf of your organization:

* Submits the Mitigation Plan, as presented, to the regional entity for acceptance and approval by NERC, and

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

Acknowledges:

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.

[redacted] 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: [redacted]

Title: [redacted]

Authorized On: October 13, 2017

Attachment 4.c
[redacted] Certification of Mitigation Plan Completion
dated May 13, 2019

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): WECC2017018458
Mitigated Standard Requirement(s): CIP-007-6 R2.
Scheduled Completion as per Accepted Mitigation Plan: May 15, 2019
Date Mitigation Plan completed: May 13, 2019
WECC Notified of Completion on Date: May 13, 2019
Entity Comment: [redacted]

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	See [redacted] for [redacted] Mitigation Plan Completion.	30,932,170

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 4.d
WECC's Verification of Mitigation Plan Completion for violation of
CIP-007-6 R2 dated January 22, 2020

From: noreply@oati.net
Sent: 01/22/2020 15:24:43
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: WECC2017018458
Standard/Requirement: CIP-007-6 R2.
Subject: Completed Mitigation Plan Acceptance

WECC received the Certification of Mitigation Plan Completion submitted by [redacted] on 05/13/2019 for the violation of CIP-007-6 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

[OATI Information - Email Template: MitPlan_Completed]