August 29, 2019

VIA ELECTRONIC FILING

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by [redacted] (the Entity), NERC Registry ID# [redacted],[2] with information and details regarding the nature and resolution of the violations[3] discussed in detail in the Settlement Agreement, attached hereto (Attachment 1), 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)).[4]

NERC is filing this Notice of Penalty because the 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 violations of CIP-007-1 and CIP-010-2 by the Entity.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation,* Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2017). *Mandatory Reliability Standards for the Bulk-Power System,* FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

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

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

The Entity agreed to the two million, one hundred thousand dollars ($2,100,000) penalty, in addition to other 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,[5] NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on these violations is set forth in the Settlement Agreement and herein.

[5] 18 C.F.R. § 39.7 (2019).

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
WECC2018019480	CIP-007-1	R2	Medium/ Severe	[redacted]	SR 4/3/18	7/22/09-3/31/17	Serious	
WECC2017017880	CIP-007-1	R3	Lower/ Severe	[redacted]	SR 6/30/17	7/22/09-9/5/17	Serious	
WECC2017017881	CIP-007-1	R5	Medium/ Severe	[redacted]	SR 6/30/17	7/22/09-11/4/16	Serious	
WECC2017017882	CIP-007-1	R6	Medium/ Severe	[redacted]	SR 6/30/17	7/22/09-7/31/17	Serious	$2.1M
WECC2018019481	CIP-007-1	R8	Medium/ Severe	[redacted]	SR 4/3/18	7/22/09-6/16/17	Moderate	
WECC2017017883	CIP-010-2	R1	Medium/ High	[redacted]	SR 6/30/17	7/1/16-3/31/17	Serious	
WECC2017017884	CIP-010-2	R2	Medium/ Severe	[redacted]	SR 6/30/17	8/5/16-6/29/17	Serious	

Background to the Violations

In 2009, the Entity installed [redacted] servers subject to CIP requirements. Each server included a [redacted], which enables [redacted]. The Entity correctly designated the [redacted] servers as Critical Cyber Assets (CCAs) that required specific protections included in the CIP Standards. However, the Entity did not recognize that the [redacted] needed to have the CIP Standards applied to them separately and directly, apart from the [redacted] servers. At the transition to the CIP Version 5

Reliability Standards, [redacted] remained installed within the Entity's High Impact Bulk Electric System (BES) Cyber Systems and Medium Impact BES Cyber Systems.

On June 30, 2017, the Entity submitted five Self-Reports stating that it was in violation of CIP-007-1 R3, R5, R6, and CIP-010-2 R1, and R2. After reviewing and analyzing all relevant information, WECC determined that, in addition to the five Self-Reports submitted by the Entity, it was also in violation of CIP-007-1 R2 and R8. The details of each violation are explained below.

WECC determined that the root cause of the violations was insufficient procedures to identify that the [redacted] were CCAs requiring separate protections under the CIP Reliability Standards. The Entity did not use the documentation tools it developed to ensure that the [redacted] of the [redacted] servers had the applicable CIP protections.

CIP-007-1 R2

WECC determined that the Entity failed to ensure that only those ports and services of its CCAs required for normal and emergency operations were enabled.

WECC determined that this violation posed a serious and 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. A copy of the Mitigation Plan is included as Attachment 2b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of October 31, 2018. Attachments 2c and 2d provide specific information on verification of the Entity's completion of the activities.

CIP-007-1 R3

WECC determined that the Entity failed to, either separately or as a component of the documented configuration management process specified in CIP-003 R6, establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

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. A copy of the Mitigation Plan is included as Attachment 3b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of July 6, 2018. Attachments 3c and 3d provide specific information on verification of the Entity's completion of the activities.

CIP-007-1 R5

The Entity failed to ensure the technical and procedural controls that enforce access authentication of and accountability for all user activity.

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 failed to establish, implement, and document technical and procedural controls that minimize the risk of unauthorized system access.

The Entity submitted its Mitigation Plan to address the referenced violation. A copy of the Mitigation Plan is included as Attachment 4b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of October 4, 2018. Attachments 4c and 4d provide specific information on verification of the Entity's completion of the activities.

CIP-007-1 R6

The Entity failed ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

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. A copy of the Mitigation Plan is included as Attachment 5b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of October 4, 2018. Attachments 5c and 5d provide specific information on verification of the Entity's completion of the activities.

CIP-007-1 R8

The Entity failed to perform a Cyber Vulnerability Assessment (CVA) of all Cyber Assets within the ESP, at least annually.

WECC determined that this violation posed a moderate 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. A copy of the Mitigation Plan is included as Attachment 6b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of October 12, 2018. Attachments 6c and 6d provide specific information on verification of the Entity's completion of the activities.

CIP-010-2 R1

The Entity failed to develop a baseline configuration for the [redacted], individually or by group.

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. A copy of the Mitigation Plan is included as Attachment 7b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of June 29, 2018. Attachments 7c and 7d provide specific information on verification of the Entity's completion of the activities.

CIP-010-2 R2

The Entity failed to monitor for changes to the baseline configuration of the [redacted] at least once every 35 calendar days.

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. A copy of the Mitigation Plan is included as Attachment 8b.

The Entity certified completion of the Mitigation Plan. WECC verified the Entity completed the Mitigation Plan as of June 29, 2018. Attachments 8c and 8d provide specific information on verification of the Entity's completion of the activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two million, one hundred thousand dollars ($2,100,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. The Entity accepted responsibility for and admitted to these violations;
2. WECC considered the Entity's compliance history an aggravating factor in determining the penalty. The Entity has prior violations of CIP-007 R2, R3, R5, R6, and R8; and CIP-010 R1;[6]
3. One violation posed a moderate risk and six violations posed a serious risk to the reliability of the BPS;
4. There was no evidence of any attempt to conceal the violations nor evidence of intent to do so; and
5. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two million, one hundred thousand dollars ($2,100,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the violations on August 14, 2019 and approved the resolution between WECC and the

[6] The Entity's relevant prior noncompliance with CIP-007 R2, R3, R5, R6, and R8; and CIP-010 R1 includes: [redacted].

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

Entity. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two million, one hundred thousand dollars ($2,100,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

For the reasons discussed below, NERC is requesting nonpublic treatment of certain portions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released 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.[9]

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

[9] 18 C.F.R. § 388.113(e)(1).

publicly disclosed.[10] The redacted information 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 its cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of the Entity, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."[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. The Redacted Portions of this Filing Should Also be Treated as CEII as the Information Could be Useful to a Person Planning an Attack on Critical Electric Infrastructure

In addition to the provisions of Section 39.7(b)(4), the redacted information also separately qualifies for treatment as CEII under Section 388.113 of the Commission's regulations. CEII is defined, in relevant part, as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: (1) relates details about the production, generation, transmission, or distribution of energy; and (2) could be useful to a person planning an attack on critical infrastructure. As discussed above, this filing includes vulnerability and design information that could be

[10] NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation. To date, the Commission has directed public disclosure regarding the disposition of CIP violations in a small number of cases. *See* Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-019 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019); and FOIA No. FY19-030, Determination on Docket No. NP10-132 (April 26, 2019). Based on the facts specific to those cases, the Commission directed public disclosure of the identity of the registered entity; the Commission did not disclose other details regarding the CIP violations.

[11] Order No. 672 at P 538.

[12] See the next section for a list of this information.

[13] See below for a list of this information.

useful to a person planning an attack on the Entity's critical infrastructure. The incapacity or destruction of the Entity's systems and assets would negatively affect national security, economic security, and public health and safety. For example, this Notice of Penalty includes the identification of a specific cyber security issue and related vulnerabilities, as well as details concerning the types and configurations of the Entity's systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

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

1. BES Cyber System Information, including security procedures; information related to BES Cyber Assets; individual IP addresses with context; group of IP addresses; and security information regarding BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, or Electronic Access Control and Monitoring Systems that is not publicly available, 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.

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 29, 2019. Details about the Entity's operations, networks, and security should be treated and evaluated separately from its identity to avoid unnecessary disclosure of CEII that could pose a risk to security. NERC requests that the CEII designation apply to the redacted information from Items 3-9 for three years from this filing date, August 29, 2019. NERC requests the CEII designation for three years to allow for several activities that should reduce the risk to the security of the BPS. Those activities include, among others:

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

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

Attachments to be Included as Part of this Notice of Penalty

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

1. Settlement Agreement by and between WECC and the Entity executed May 6, 2019, included as Attachment 1;
2. The Entity's Self-Report of violation of CIP-007-1 R2 submitted April 3, 2018, included as Attachment 2a;
3. The Entity's Mitigation Plan designated as WECCMIT014130 for CIP-007-1 R2 submitted September 13, 2018, included as Attachment 2b;
4. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R2 submitted November 9, 2018, included as Attachment 2c;
5. Verification of Mitigation Plan Completion for CIP-007-1 R2 dated January 24, 2019, included as Attachment 2d.
6. The Entity's Self-Report of violation of CIP-007-1 R3 submitted June 30, 2017, included as Attachment 3a;
7. The Entity's Mitigation Plan designated as WECCMIT013254-2 for CIP-007-1 R3 submitted August 9, 2018, included as Attachment 3b;
8. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R3 submitted October 30, 2018, included as Attachment 3c;
9. Verification of Mitigation Plan Completion for CIP-007-1 R3 dated October 31, 2018, included as Attachment 3d.
10. The Entity's Self-Report of violation of CIP-007-1 R5 submitted June 30, 2017, included as Attachment 4a;
11. The Entity's Mitigation Plan designated as WECCMIT013366-1 for CIP-007-1 R5 submitted August 9, 2018, included as Attachment 4b;
12. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R5 submitted October 5, 2018, included as Attachment 4c;
13. Verification of Mitigation Plan Completion for CIP-007-1 R5 dated January 18, 2019, included as Attachment 4d.
14. The Entity's Self-Report of violation of CIP-007-1 R6 submitted June 30, 2017, included as Attachment 5a;

15. The Entity's Mitigation Plan designated as WECCMIT013255-1 for CIP-007-1 R6 submitted May 29, 2018, included as Attachment 5b;
16. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R6 submitted October 5, 2018, included as Attachment 5c;
17. Verification of Mitigation Plan Completion for CIP-007-1 R6 dated January 18, 2019, included as Attachment 5d.
18. The Entity's Self-Report of violation of CIP-007-1 R8 submitted April 3, 2018, included as Attachment 6a;
19. The Entity's Mitigation Plan designated as WECCMIT014136 for CIP-007-1 R8 submitted September 18, 2018, included as Attachment 6b;
20. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R8 submitted October 16, 2018, included as Attachment 6c;
21. Verification of Mitigation Plan Completion for CIP-007-1 R8 dated January 24, 2019, included as Attachment 6d.
22. The Entity's Self-Report of violation of CIP-010-2 R1 submitted June 30, 2017, included as Attachment 7a;
23. The Entity's Mitigation Plan designated as WECCMIT013348-1 for CIP-010-2 R1 submitted June 25, 2018, included as Attachment 7b;
24. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R1 submitted July 31, 2018, included as Attachment 7c;
25. Verification of Mitigation Plan Completion for CIP-010-2 R1 dated September 14, 2018, included as Attachment 7d.
26. The Entity's Self-Report of violation of CIP-010-2 R2 submitted June 30, 2017, included as Attachment 8a;
27. The Entity's Mitigation Plan designated as WECCMIT013256-1 for CIP-010-2 R2 submitted August 9, 2018, included as Attachment 8b;
28. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted August 13, 2018, included as Attachment 8c;
29. Verification of Mitigation Plan Completion for CIP-010-2 R2 dated September 18, 2018, included as Attachment 8d.

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

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 *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.	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Alexander Kaplen* Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile alexander.kaplen@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/ Alexander Kaplen

Edwin G. Kichline
Senior Counsel and Director of
Enforcement Oversight
Alexander Kaplen
Associate Counsel
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net
alexander.kaplen@nerc.net

cc: The Entity
Western Electricity Coordinating Council

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

Attachment 1

Settlement Agreement by and between WECC and
The Entity executed May 6, 2019

[redacted]

WECC
Electric Reliability and Security for the West

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

April 29, 2019

[redacted]

Subject: Notice of Expedited Settlement Agreement

[redacted]

I. Introduction

The Western Electricity Coordinating Council (WECC) hereby notifies [redacted] that WECC identified Possible Violations of North American Electric Reliability Corporation (NERC) Reliability Standards (Reliability Standards) in the Preliminary Screen process and 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 penalty and/or sanctions 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-007-1 R2	WECC2018019480	WECC2018-614883
CIP-007-1 R3	WECC2017017880	WECC2017-614570
CIP-007-1 R5	WECC2017017881	WECC2017-614571
CIP-007-1 R6	WECC2017017882	WECC2017-614572
CIP-007-1 R8	WECC2018019481	WECC2018-614882
CIP-010-2 R1	WECC2017017883	WECC2017-614573
CIP-010-2 R2	WECC2017017884	WECC2017-614574

The attached Expedited Settlement Agreement includes a summary of the facts and evidence supporting each Alleged Violation, as well as the basis on which the penalty and/or sanctions were determined.

III. Proposed Penalty or Sanction

Pursuant to the Federal Energy Regulatory Commission's (FERC or Commission) regulations and orders, NERC Rules of Procedure, and the NERC Sanction Guidelines, WECC proposes to assess a penalty for the violations of the Reliability Standards referenced in the Attachment in the amount of $2,100,000.

In determining a penalty and/or sanction, WECC considers various factors that may include, but are not limited to: (1) Violation Risk Factor; (2) Violation Severity Level; (3) risk to the reliability of the Bulk Electric System (BES)[1], including the seriousness of the violation; (4) Violation Time Horizon and timeliness of remediation; (5) the violation's duration; (6) the Registered Entity's compliance history; (7) the timeliness of the Registered Entity's self-report; (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 Internal 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; (13) whether the Registered Entity admits to and takes responsibility for the violation; (14) "above and beyond" actions and investments made by the

[1] "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))

Registered Entity in an effort to prevent recurrence of this issue and/or proactively address and reduce reliability risk due to similar issues; and (15) the Registered Entity's ability to pay a penalty, as applicable.

WECC's determination of penalty is guided by the statutory requirement codified at 16 U.S.C. § 824o(e)(6) that any penalty imposed "shall bear a reasonable relation to the seriousness of the violation and shall take into consideration the efforts of [the Registered Entity] to remedy the violation in a timely manner." In addition, WECC considers all other applicable guidance from NERC and FERC.

IV. Procedures for Registered Entity's Response

If [redacted] accepts WECC's proposal that the violations listed in the Settlement Agreement be processed through the Expedited Settlement process, [redacted] must sign the attached Settlement Agreement and submit it through the WECC Enhanced File Transfer (EFT) Server Enforcement folder **within 10 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 10 calendar days from the date of this Notice**, informing WECC of the decision not to accept WECC's proposal.

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 representative from [redacted] 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.

April 29, 2019

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 801-819-7610 or dhorvath@wecc.org.

Sincerely,

Heather M. Laws
Director, Enforcement

Cc: NERC Enforcement

Attachment

EXPEDITED SETTLEMENT AGREEMENT

OF

WESTERN ELECTRICITY COORDINATING COUNCIL

AND

[redacted]

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

1. [redacted] admits to 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. The terms of this Settlement Agreement, including the agreed upon payment, are subject to review and possible revision by NERC and FERC. Upon NERC approval of the Settlement Agreement, NERC will file a Notice of Penalty with FERC and will post the Settlement Agreement 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.

4. 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.

5. This Settlement Agreement represents a full and final disposition of the violations listed below, [redacted] and further 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.

6. In the event [redacted] fails to comply with any of the terms set forth in this Settlement Agreement, WECC will initiate enforcement, penalty, and/or sanction actions against [redacted] to the maximum extent allowed by the NERC Rules of Procedure, up to the maximum statutorily allowed penalty. Except as otherwise specified in this Settlement Agreement, [redacted] shall retain all rights to defend against such enforcement actions, in accordance with the NERC Rules of Procedure.

7. This Settlement Agreement shall be governed by and construed under federal law.

8. 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.

9. 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 that Party's behalf [redacted].

10. The undersigned representative of each Party affirms that he or she has read the Settlement Agreement, that all representations 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 each Party in express reliance on those representations.

11. [redacted]

12. In addition, [redacted] must submit Mitigation Plans <u>within 30 calendar days</u> from the date of this Settlement Agreement, if it has not already done so previously.

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

A. **NERC RELIABILITY STANDARDS:**
CIP-007-1 REQUIREMENTS R2, R3, R5, R6, R8 AND CIP-010-2 REQUIREMENTS R1, R2
NERC VIOLATION IDS:
WECC2018019480, WECC2017017880, WECC2017017881, WECC2017017882, WECC2018019481, WECC2017017883, WECC2017017884
WECC VIOLATION IDS:
WECC2018-614883, WECC2017-614570, WECC2017-614571, WECC2017-614572, WECC2018-614882, WECC2017-614573, WECC2017-614574,

RELIABILITY STANDARDS

14. NERC Reliability Standards CIP-007-1 Requirements R2, R3, R5, R6, R8, and CIP-010-2 R1, R2 states:

CIP-007-1 R2, R3, R5, R6, R8*:*

R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

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

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for,

all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-010-2 R1, R2:

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.

Part 1.1 Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

1.1.3. Any custom software installed;

1.1.4. Any logical network accessible ports; and

1.1.5. Any security patches applied.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.

Part 2.1 Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

STIPULATED VIOLATION FACTS

15. On June 30, 2017, the entity submitted five Self-Reports stating that, as a [redacted] it was in violation of CIP-007-1 R3, R5, R6, and CIP-010-2 R1, and R2.

16. Specifically, the entity reported that in 2009 it installed [redacted] servers which it identified as Critical Cyber Assets (CCAs) under CIP Version 1 that were associated with the entity's Energy Management System (EMS), Remedial Action Schemes (RAS) and Supervisory Control and Data Acquisition (SCADA) systems. These CCAs were located in the entity's primary and backup [redacted] Control Centers, Data Center, Operations Center and [redacted] Substations. At the time the [redacted] servers were installed, the entity overlooked that each server included a [redacted] as the CIP Requirements were being applied to the servers.

17. The [redacted] allowed [redacted] into the [redacted] server to provide the entity's [redacted] on the server. The [redacted] was essential to the reliable operation of the [redacted] server to which it was connected; had External Routable Connectivity (ERC); and had one port which was physically connected externally to allow a [redacted] The [redacted] also [redacted] the [redacted] server.

18. The entity stated that it understood the [redacted] to be the same device as the [redacted] server; therefore, it concluded that if the server had the protective measures of the CIP Standards and Requirements for a CCA, then the [redacted] did as well. The entity did not realize that given the way the [redacted] was designed, configured, and implemented required it to have the CIP Standards and Requirements applied to it separately and directly, apart from the [redacted] server. As a result, the entity did not prepare a separate formal "configuration manual" that included instructions regarding the security settings for the [redacted] that would have ensured it was compliant with the applicable CIP Standards and Requirements. Additionally, the entity's Cyber Asset On-Boarding [redacted] did not include checks or steps to account for the [redacted] of the [redacted] server. As the CIP Standards were updated to Version 5 and became mandatory and enforceable, [redacted] servers with [redacted] remained installed within the entity's High Impact BES Cyber Systems (HIBCS) and [redacted] servers with [redacted] remained installed within its Medium Impact BES Cyber Systems (MIBCS).

19. After reviewing and analyzing all relevant information, WECC determined that in addition to the five Self-Reports submitted by the entity, it was also in violation of CIP-007-1 R2 and R8. The specific failure of each Standard and Requirement by the entity as it pertains to the [redacted] of the [redacted] server are detailed as follows. The entity failed to:
    a. ensure that only those ports and services required for normal and emergency operations were enabled, as required by CIP-007-1 R2 (WECC2018019480);
    b. either separately or as a component of the documented configuration management process specified in CIP-003 R6, ensure security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP, as required by CIP-007-1 R3 (WECC2017017880);
    c. ensure the technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access, as required by CIP-007-1 R5 (WECC2017017881);
    d. ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security, as required by CIP-007-1 R6 (WECC2017017882);
    e. perform a Cyber Vulnerability Assessment (CVA) of all Cyber Assets within the ESP at least annually, as required by CIP-007-1 R8 (WECC2018019481);
    f. develop a baseline configuration, individually or by group, which included; firmware where no independent operating system exited; any logical network accessible ports; and any security patches applied, as required by CIP-010-2 R1 Part 1.1, Sub-Parts 1.1.1, 1.1.4, and 1.1.5 (WECC2017017883); and
    g. monitor at least once every 35 calendar days for changes to the baseline configuration, as required by CIP-010-2 R2 Part 2.1 (WECC2017017884);

20. The root cause of these violations was the entity failing to realize that the [redacted] design, configuration, and implementation required the entity to apply specific CIP Standards and Requirements to the [redacted] separately, apart from the [redacted] server. Therefore, the entity did not utilize the documentation tools it had developed to ensure that the [redacted] of the [redacted] server was afforded the appropriate and applicable CIP protections.

21. WECC determined the violations started and ended as described in Table 1.

Table 1

Standard and Requirement	NERC Violation ID	Start Date	End Date	Violation Duration in days
CIP-007-1 R2	WECC2018019480	7/22/2009	3/31/2017	2,810
CIP-007-1 R3	WECC2017017880	7/22/2009	9/5/2017	2,968
CIP-007-1 R5	WECC2017017881	7/22/2009	11/4/2016	2,663
CIP-007-1 R6	WECC2017017882	7/22/2009	7/31/2017	2,932
CIP-007-1 R8	WECC2018019481	7/22/2009	6/16/2017	2,887
CIP-010-2 R1	WECC2017017883	7/1/2016	3/31/2017	274
CIP-010-2 R2	WECC2017017884	8/5/2016	6/29/2017	328

RELIABILITY RISK ASSESSMENT

22. WECC determined that these violations posed a serious or substantial risk to the reliability of the Bulk Power System (BPS).

23. In these instances, for the [redacted] servers with [redacted], the entity failed to:
    a. establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled, as required by CIP-007-1 R2;
    b. either separately or as a component of the documented configuration management process specified in CIP-003 R6, establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s) (ESP), as required by CIP-007-1 R3;
    c. establish, implement, and document technical and procedural controls that enforce access authentication of and accountability for all user activity, and that minimize the risk of unauthorized system access, as required by CIP-007-1 R5;
    d. ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security, as required by CIP-007-1 R6;
    e. perform a CVA of all Cyber Assets within the ESP at least annually which includes a document identifying the vulnerability assessment process; a review to verify that only ports and services required for operations are enabled; a review of controls for default accounts; and documentation of the results of the assessment, as required by CIP-007-1 R8,

24. In these instances, for the [redacted] servers with [redacted], the entity failed to:
    a. develop a baseline configuration, individually or by group, which shall include the following items: R1.1.1; operating system or firmware where no independent operating system exists. R1.1.4. any logical network accessible ports; and R1.1.5; any security patches applied, as required by CIP-010-2 R1; and
    b. monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1 of CIP-010-2), as required by CIP-010-2 R2.

25. The entity implemented weak preventative controls. Specifically, a separation of duties was in place to perform the initial Cyber Asset configuration tasks and an onboarding device [redacted] for new Cyber Assets. However, the [redacted] were not included in the onboarding [redacted] for new Cyber Assets. The entity also had an in-depth Change Management Training Program that included a Cyber Vulnerability Assessment. However, the [redacted] were not included in that program.

26. The entity implemented weak detective controls. Specifically, a SEIM system that was designed to track baseline configurations of CIP Cyber Assets was installed and would run a scan of all Cyber Assets to verify which ones required an initial baseline configuration or an updated baseline due to a change. However, the [redacted] were not included in the SEIM system. Lastly, because the entity did not implement security event logging for the [redacted], it would not have been alerted of any related security events.

27. The entity implemented a good compensating control. The entity had a corporate firewall located between the remote users and the ESP where the [redacted] servers with the [redacted] resided, which limited the ability of a malicious attack from outside. The [redacted] servers on which the [redacted] resided had security patching; had malicious software prevention; had baseline configuration documentation; had CVA's; and had documentation to show which ports and services where enabled and determined necessary, where applicable. Nevertheless, no harm is known to have occurred.

DESCRIPTION OF REMEDIATION AND MITIGATION

28. The entity submitted Mitigation Plans to address these violations as stated in Table 2.

Table 2

Standard and Requirement	NERC Violation ID	Mitigation Plan Submittal Date	Date Mitigation Plan Accepted by WECC
CIP-007-1 R2	WECC2018019480	9/13/2018	9/13/2018
CIP-007-1 R3	WECC2017017880	8/09/2018	8/09/2018
CIP-007-1 R5	WECC2017017881	8/09/2018	8/9/2018
CIP-007-1 R6	WECC2017017882	5/29/2018	6/07/2018
CIP-007-1 R8	WECC2018019481	9/18/2018	9/26/2018
CIP-010-2 R1	WECC2017017883	6/25/2018	6/25/2018
CIP-010-2 R2	WECC2017017884	8/09/2018	8/09/2018

29. To remediate the CIP-007-1 R2 violation, the entity:
    a. updated [redacted] server baseline configurations to include all [redacted] attributes;
    b. trained applicable system administrators on the [redacted] updates and requirements for compliance;
    c. created a [redacted] configuration script to apply the [redacted];
    d. updated its Patch Cycle User Guide;
    e. created a "5 Minute Meeting" training document as a method for training personnel on the additional controls (script and patch cycle guide); and
    f. trained personnel on the new controls.

30. To remediate the CIP-007-1 R3 violation, the entity:
    a. applied updated firmware on the [redacted] in scope;
    b. updated documentation to include its new process for tracking, evaluating, and installing firmware updates on all [redacted]; and
    c. provided training to applicable personnel on its updated documentation and processes.

31. To remediate the CIP-007-1 R5 violation, the entity:
    a. updated the shared admin password on the [redacted] in scope;
    b. updated documentation to include its new process the system access controls for all [redacted]; and
    c. provided training to applicable personnel on its updated documentation and processes.

32. To remediate the CIP-007-1 R6 violation, the entity:
    a. created and test script to configure the [redacted] to send logs to its enterprise logging system;
    b. disabled [redacted] due to incorrect licenses and therefore cannot be configured to log, age of the [redacted] therefore are not capable of logging

through the enterprise logging system, and an unknown cause for one [redacted] that is not logging;

c. updated documentation to include its new process for security event monitoring for all [redacted];

d. provided training to applicable personnel on its updated documentation and processes

33. To remediate the CIP-007-1 R8 violation, the entity:

a. performed CVAs on the [redacted];

b. updated [redacted] server baseline configurations to include all [redacted] attributes;

c. created, approved, and published a [redacted] Manual;

d. configured its asset management tool to display a listing of [redacted];

e. updated and published its Cyber Security Vulnerability Assessment Procedure to include language for [redacted];

f. trained applicable system administrators on the [redacted] updates and requirements for compliance; and

g. performed 2018 CVAs in accordance with its updated procedure to ensure inclusion of the [redacted].

34. To remediate and mitigate the CIP-010-2 R1 violation, the entity:

a. updated its [redacted] server baseline configurations to include all [redacted] attributes;

b. updated its [redacted] OS Cyber Assets on-boarding [redacted] to include [redacted] and

c. updated its configuration change management procedure to include specific notes about enumeration of lights-out or out-of-band management interfaces that may be part of the [redacted] server hardware; and

d. provided training to applicable personnel on its updated documentation and processes.

35. To remediate and mitigate the CIP-010-2 R2 violation, the entity:

a. automated configuration monitoring in its SEIM for the those [redacted] associated with its HIBCS that can be automated;

b. implemented a manual process for the [redacted] that cannot be monitored in the SEIM;

c. confirmed output from the SEIM contained firmware version; baseline configurations; and ports and services;

d. updated its [redacted] OS Cyber Assets on-boarding [redacted] to include [redacted];

e. updated documentation to include its new process for automated manual configuration monitoring for applicable [redacted]; and

f. provided training to applicable personnel on its updated documentation and processes.

36. To mitigate the root cause and address future prevention for all the violations, the entity:
    a. created, approved, and published a [redacted] Manual;
    b. configured its asset management tool to display a listing of [redacted];
    c. updated its "[redacted] OS Cyber Asset On-Boarding [redacted] to include [redacted]

37. The entity submitted Mitigation Plan Completion Certifications as stated in Table 3.

Table 3

Standard and Requirement	NERC Violation ID	CMP Certification Date	Date CMP Verified by WECC
CIP-007-1 R2	WECC2018019480	11/9/2018	1/24/2019
CIP-007-1 R3	WECC2017017880	10/30/2018	10/31/2018
CIP-007-1 R5	WECC2017017881	10/5/2018	1/18/2019
CIP-007-1 R6	WECC2017017882	10/5/2018	1/18/2019
CIP-007-1 R8	WECC2018019481	10/16/2018	1/24/2019
CIP-010-2 R1	WECC2017017883	7/31/2018	9/14/2018
CIP-010-2 R2	WECC2017017884	8/13/2018	9/18/2018

PROPOSED PENALTY OR SANCTION

38. WECC determined that the proposed penalty of $2,100,000 is appropriate for the following reasons:
    a. Base penalty factors:
        i. The VRF and the VSL are as stated in Table 4.

Table 4

Standard and Requirement	NERC Violation ID	VRF	VSL
CIP-007-1 R2	WECC2018019480	Medium	Severe
CIP-007-1 R3	WECC2017017880	Lower	Severe
CIP-007-1 R5	WECC2017017881	Medium	Severe
CIP-007-1 R6	WECC2017017882	Medium	Severe
CIP-007-1 R8	WECC2018019481	Medium	Severe
CIP-010-2 R1	WECC2017017883	Medium	High
CIP-010-2 R2	WECC2017017884	Medium	Severe

        ii. The violation duration for CIP-007-1 R2, R3, R5, R6, and R8 is 2,810, 2,968, 2,663, 2,932, and 2,887 days, respectively, as described above in Section 8. However,

Requirements 2 and 8 have an Operations Assessment violation time horizon expectation for remediation within 30 days to preserve the reliability of the BPS. Requirements 3 and 6 have a Long-Term Planning violation time horizon expectation for remediation within one year to preserve the reliability of the BPS. Requirement 5 has a Real-Time Operations violation time horizon expectation for remediation for actions required within one hour or less to preserve the reliability of the BPS. The entity did not have any detective controls in place that could have helped identify the issues sooner to lessen the extensive violation duration and thereby lessen the risk to the BPS.

iii. The violation duration for CIP-010-2 R1 and CIP-010-2 R2 was 274 and 364 days, respectively, as described above in Section 8. However, these two Requirements have an Operations Planning violation time horizon expectation for remediation within the next day, up to and including the quarter, to preserve the reliability of the BPS. The entity did not have any detective controls in place that could have helped identify the issues sooner to lessen the extensive violation duration and thereby lessen the risk to the BPS.

iv. The CIP-007-1 R8 violation posed a moderate risk to the reliability of the BPS. All other violations posed a serious and substantial risk to the reliability of the BPS. However, given the significance of the potential impact of the overall issue, the entire case has been assessed as posing a serious and substantial risk to the reliability and security of the BPS.

b. WECC applied a mitigating credit for the following reasons:
   i. The entity accepted responsibility and admitted to the violation.
   ii. The entity agreed to settle these violations and penalty.

c. WECC considered the entity's compliance history to be an aggravating factor.
   i. The entity's compliance history related to CIP-007-1, given NERC Violation ID's [redacted], and the compliance history related to CIP-010-2 given NERC Violation ID [redacted], was relevant and applicable to the violations in this Notice.

d. Other Considerations:
   i. WECC considered the entity's compliance history for CIP-007-1 and CIP-010-2 and determined that the some of the entity's prior noncompliance was distinct, separate, and not relevant to the violations in this Notice. For NERC Violation IDs

[redacted], [redacted], [redacted], and [redacted] the entity failed to submit Technical Feasibility Exceptions. For NERC Violation ID [redacted] and [redacted], the entity failed to document evidence.

ii. WECC did not give Self-Reporting credit for WECC2017017880, WECC2017017881, WECC2017017882, WECC2017017883, and WECC2017017884 due to the length of time between the discovery day and the Self-Report date being between 328 and 649 days. WECC views such a time delay as the entity not having a strong culture of compliance. Additionally, WECC did not apply mitigating credit for Self-Reporting WECC2018019480 and WECC2018019481 as the entity submitted those Self-Reports at the request of WECC.

iii. WECC did not apply mitigating credit for the entity's Internal Compliance Program (ICP). Although the entity has a documented ICP, WECC determined that the entity did not implement its ICP with effective internal controls sufficient to identify, assess, report, and mitigate these violations in a timely manner, thereby reducing the risk to the BPS. This was evident by the duration between the discovery date and the Self-Report submittal date, which is indicative of an insufficient or ineffective ICP.

iv. WECC did not apply a mitigating credit for cooperation. The entity did not quickly address the violations; determine the facts, and report mitigation. This is evident by the duration between the Self-Report submittal date and the Mitigation Plan submittal date as described in Table 5. WECC repeatedly requested information from the entity and the entity was indifferent both in time and with information when responding to those requests.

Table 5

Standard and Requirement	NERC Violation ID	Self-Report Submittal Date	Mitigation Plan Submittal Date	Duration in Days
CIP-007-1 R2	WECC2018019480	4/3/2018	9/13/2018	163
CIP-007-1 R3	WECC2017017880	6/30/2017	8/9/2018	405
CIP-007-1 R5	WECC2017017881	6/30/2017	8/9/2018	405
CIP-007-1 R6	WECC2017017882	6/30/2017	5/29/2018	333
CIP-007-1 R8	WECC2018019481	4/3/2018	9/18/2018	168
CIP-010-2 R1	WECC2017017883	6/30/2017	6/25/2018	360
CIP-010-2 R2	WECC2017017884	6/30/2017	8/9/2018	405

v. WECC did not apply mitigating credit for admitting to these violations because the entity has historically chosen to neither admit or deny in settlement. However, should the entity choose to settle these violations and admit responsibility for their actions, credit may be applied against the overall proposed penalty.

vi. Upon undertaking the actions outlined in the Mitigation Plan, the entity took voluntary corrective action to remediate this violation.

vii. The entity did not fail to complete any applicable compliance directives. There was no evidence of any attempt by the entity to conceal these violations. There was no evidence that the violations were intentional.

e. WECC determined there were no other aggravating factors warranting a penalty higher than the proposed penalty.

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

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

Attachment 2

2a. The Entity's Self-Report of violation of CIP-007-1 R2 submitted April 3, 2018

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-1

Requirement: CIP-007-1 R2.

Date Submitted: April 03, 2018

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 22, 2009

End/Expected End Date:

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

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: Certain [redacted] include [redacted] a component that allows for [redacted] When [redacted] installed [redacted] in 2009, [redacted] overlooked the fact that some of its [redacted] included [redacted]. As a result, [redacted] initially failed to prepare a formal configuration manual that included instructions on the security settings for the [redacted] to show which ports and services were enabled and determined necessary. Additionally, [redacted] Cyber Asset On-Boarding [redacted] did not include checks or steps to account for the [redacted] of the physical servers. This lack of configuration documentation and asset verification led to inconsistent configuration of physical servers throughout the [redacted] enterprise.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Updated [redacted] baseline configurations to include all [redacted] attributes on 3/31/2017. [redacted] team developed a configuration manual in September 2017. That same team made revisions, in July 2017 to [redacted] to include [redacted] in order to facilitate the verification process. Both mitigation actions support the server component inclusion function of

configuration and change management.

Have Mitigating Activities been Completed? Yes

Date Mitigating Activities Completed: September 27, 2017

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Unauthorized access to [redacted] could result in a loss of [redacted]

Risk Assessment of Impact to BPS: Minimal, because [redacted] would be promptly notified of the loss of [redacted] from unauthorized access, and could restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	[redacted] Configuration Manual approved 9/27/2017. Manual is in the process of being revised to correct format.	249,120
Entity	[redacted]	[redacted] Configuration Manual Approval document.	67,450
Entity	[redacted]	Updated [redacted] Cyber Assets On-boarding [redacted] Update included [redacted] on [redacted]	188,495

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

Attachment 2

2b. The Entity's Mitigation Plan designated as WECCMIT014130 for CIP-007-1 R2 submitted September 13, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
WECC2018019480	CIP-007-1 R2.	07/19/2018

Mitigation Plan Submitted On: September 13, 2018

Mitigation Plan Accepted On: September 13, 2018

Mitigation Plan Proposed Completion Date: November 09, 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		
WECC2018019480	07/22/2009	CIP-007-1 R2.
Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.		

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

Certain [redacted] include [redacted] that allows for [redacted]
The [redacted] may be provided on [redacted] When [redacted] installed [redacted] servers in 2009, [redacted] overlooked the fact that some of its [redacted] included [redacted] components.
As a result, [redacted] initially failed to prepare a formal configuration manual that included instructions on the security settings for the [redacted] to show which ports and services were enabled and determined necessary.
Additionally, [redacted] Cyber Asset On-Boarding [redacted] did not include checks or steps to account for the [redacted] of the physical servers.
This lack of configuration documentation and asset verification led to inconsistent configuration of physica[redacted] throughout the [redacted] enterprise.

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

WECC notified [redacted] of the violation after reviewing the other [redacted] Self Reports.

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:

In 2017, [redacted] included [redacted] to be a part of the [redacted] baseline configuration (CIP-010 R1.1) including the respective ports and services used by [redacted] and the justifications for enabled ports. A configuration manual was created and published for [redacted] Instructions for configuring [redacted] were added to the [redacted] Server [redacted] and training was completed to respective administrators on the change. Steps are being taken to implement controls to monitor and report compliance of [redacted] configuration for prevention of future noncompliance.

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

Proposed Completion date of Mitigation Plan: November 09, 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
Milestone1: Update baseline configurations	Updated [redacted] baseline configurations to include all [redacted] Attributes. The baseline configurations are where [redacted] documents the logical ports and services enabled as well as the justification of need for each port.	03/31/2017	03/31/2017	This milestone is complete. In accordance with [redacted] Configuration Change Management, the [redacted] have been documented in a baseline configuration.	No
Milestone1a:	placeholder to extent time between milestones	06/30/2017	06/30/2017		No
Milestone 2: Create [redacted] Configuration Manual	[redacted] team developed a configuration manual in September 2017 called [redacted]	07/31/2017	07/31/2017	[redacted] has verified that the milestone is completed.	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
	[redacted]. The configuration manual is used by the System admins during the time of configuration to disable features that are not required on the[redacted]				
Milestone 3: Approve Configuration Manual	[redacted] Configuration Manual has been revised, approved, and published. Document Name: [redacted]	09/27/2017	09/27/2017	[redacted] has verified that the milestone is completed and the documentation is located in [redacted]	No
Milestone 3a	Time placeholder	12/26/2017	12/26/2017		No
Milestone 4: Document [redacted] in Asset Management Tool	Configure the [redacted] to display a listing of [redacted] will be displayed on the [redacted] tab of the [redacted] NERC Portal.	02/01/2018	02/01/2018	Deployed [redacted]	No
Milestone 4a	Time Placeholder	04/23/2018	04/30/2018		No
Milestone 5: Update Asset onboarding [redacted] to include [redacted]	Update [redacted] to include [redacted] in order to facilitate the verification process for configuration [redacted] security configurations.	06/30/2018	07/05/2018	As a result of updating this procedure, we have verified that the [redacted] administrators are using the correct and approved [redacted]	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
Milestone 6: Train on [redacted]	[redacted] Training provided on the [redacted] to inform the applicable system administrators on the [redacted] updates and requirements.	07/03/2018	07/03/2018	All administrators have been trained and a log of the meeting was captured.	No
Milestone 7: Publish [redacted]	[redacted]	07/31/2018	07/31/2018	The document was published and used the following routing: [redacted]	No
Milestone 10: Training on Script and Patch User Guide	Create a 5 Minute Meeting training document as a method for training personnel on the additional controls in milestones 8 and 9. Train Personnel on the user guide.	10/31/2018			No
Milestone 8: Create [redacted] configuration Script	Create a script to apply the [redacted] configuration in accordance with the [redacted] Configuration Manual. [redacted] will run the script to apply configuration settings each patch cycle and/or utilize a configuration monitoring tool annually to check the [redacted] configuration settings are meeting Configuration Manual as referenced in Milestone 2.	10/31/2018		This action was added as a preventative measure to ensure compliance of [redacted] configuration. This will reduce potential vulnerability footprint by disabling unnecessary logical ports and services as required in CIP-007.	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
Milestone 9: Update Patch Cycle User Guide	Update the patch cycle user guide to include steps on running the [redacted] configuration script and use of the configuration monitoring tool.	10/31/2018			No

Additional Relevant Information

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.

Unauthorized access to [redacted] could result in a loss [redacted] (e.g. [redacted]
Risk Assessment of Impact: Minimal, because [redacted] would be promptly notified of the loss [redacted] from unauthorized access and could restore access.
[redacted] has now included the [redacted] as part of the compliance scope and applying protective measures as required.

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

Additional steps are being taken to utilize tools for checking Configuration Manual compliance (Milestone 8). Upon completion of this mitigation plan [redacted] will have additional detective and corrective controls to ensure the appropriate identification and configuration of [redacted].

The [redacted] are now included in the [redacted] program and the root cause of this issue was remediated in 2017. The completion of all Milestones in this Mitigation Plan will introduce additional controls to detect and prevent future instances of violations. [redacted] is adding process steps to verify and monitor the configuration setting of production [redacted] on a routine basis.

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

Measures and controls are in place to detect and prevent future instances of violations on a recurring basis as described in Milestone 8.

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: [redacted]

This assessment is being provided for this new mitigation plan.

On 08/20/2018 this RAM analyst discussed this plan with the entity.

The reviewer performed an assessment of this mitigation plan and verifies the following:

1. The entity has adequately described the non-compliance including the full scope or extent of the non-compliance.

A total [redacted] include [redacted] a [redacted] n 07/22/2009, the entity failed (CIP-007-1 R2) Ports and Services, to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations. The [redacted] deployed are part of the [redacted] at the entity NERC high and medium impact sites. [redacted] include [redacted] associated with High Impact and [redacted] associated with Medium Impact.

2. The cause of the non-compliance is identified.

The [redacted] cause was an oversight by SMEs who monitor and manage the [redacted]. This was also an oversight by Management who also did not identify the noncompliance. Additionally, as an [redacted] they are installed in, the root cause was due to not being originally recognized and documented in the onboarding [redacted] as requiring the application of the CIP requirements. SMEs and Management did not identify that the [redacted] were not in the onboarding [redacted]

3. The entity's proposed actions directly address the non-compliance and will clearly restore compliance.

Milestone1: Update baseline configurations

Updated [redacted] baseline configurations to include all [redacted] Attributes. The baseline configurations are where [redacted] documents the logical ports and services enabled as well as the justification of need for each port.

Evidence:

Milestone [redacted]

Milestone [redacted]

Milestone [redacted]

Description: The entity completed remediation for all [redacted] by adding the ports and services within the baseline configurations.

Completion Date: 03/31/2017

4. The entity's proposed actions will prevent recurrence of the non-compliance.

Milestone 2: Create [redacted] Configuration Manual

[redacted] team developed a configuration manual in September 2017 called [redacted] The configuration manual is used by the System admins during the time of configuration to disable features that are not required on the [redacted]

Milestone 3: Approve Configuration Manual

[redacted] Configuration Manual has been revised, approved, and published. Document Name: [redacted]

Milestone 4: Document [redacted] in Asset Management Tool

[redacted] to display a listing of [redacted] The [redacted] will be displayed on the [redacted] tab of the [redacted] NERC Portal.

Milestone 5: Update Asset onboarding [redacted] to include [redacted]

Update [redacted] to include [redacted] in order to facilitate the verification process for configuration [redacted] security configurations.

Milestone 6: Train on [redacted]

[redacted] Training provided on the [redacted]

[redacted] inform the applicable system administrators on the [redacted] updates and requirements.

Milestone 7: Publish [redacted]

Publish [redacted]

Milestone 8: Create [redacted] configuration Script

Create a script to apply the [redacted] configuration in accordance with the [redacted] Configuration Manual. [redacted] will run the script to apply configuration settings each patch cycle and/or utilize a configuration monitoring tool annually to check the [redacted] configuration settings are meeting Configuration Manual as referenced in Milestone 2.

Milestone 9: Update Patch Cycle User Guide

Update the patch cycle user guide to include steps on running the [redacted] configuration script and use of the configuration monitoring tool.

Milestone 10: Training on Script and Patch User Guide

Create a 5 Minute Meeting training document as a method for training personnel on the additional controls in milestones 8 and 9. Train Personnel on the user guide.

5. The plan states that all mitigating activities outlined in the plan will be completed by 10/31/2018.

The plans states that the non-compliance was remediated on 03/31/2017.

6. If the duration of the Mitigation Plan is longer than 90 days, measurable milestones are identified that are no more than 3 months apart.

The plan contains ten milestones that consist of actual remediation and mitigation activities.

There are 13 milestones in total. The remaining three are sub milestones. This was remediated on 03/31/2017. The entity has been in the process of developing and completing milestones associated with mitigation. When the entity submitted this mitigation plan, they had to add filler milestones to extend the amount of time between both remediation steps and mitigation steps. The entity did not complete major milestones every three months.

7. The entity's plan addresses actions to ensure reliability is maintained during the implementation of the Mitigation Plan.

The entity remediated the noncompliance on 03/31/2017.

The entity would be promptly notified of the loss of server functionality from unauthorized access and could restore access. The entity has now included the [redacted] as part of the compliance scope and applying protective measures as required.

[redacted]

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

Attachment 2

2c. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R2 submitted November 9, 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): WECC2018019480
Mitigated Standard Requirement(s): CIP-007-1 R2.
Scheduled Completion as per Accepted Mitigation Plan: November 09, 2018
Date Mitigation Plan completed: October 30, 2018
WECC Notified of Completion on Date: November 09, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 8 - Creation of Script.pdf	Milestone 8 - [redacted] configuration Script.	156,149
Entity	Milestone 9 patch cycle User Guide.pdf	Milestone 9: Updated patch user guide - see section 5.	695,720
Entity	Milestone 10 A five minute meeting training document.pdf	Milestone 10 has 3 evidence artifacts: 10 A) Meeting with [redacted] to discuss the five minute meeting on te [redacted] script and use during patch cycle / onboarding of new [redacted] ([redacted]). Training roster for this meeting is in artifact 10B.	876,362
Entity	Milestone 10 B Training Rosters.pdf	Milestone 10 has 3 artifacts: 10 B) 2 Training Rosters for 2 separate meetings. 1. [redacted] meeting; 2. Administrator's Weekly Huddle session.	198,787
Entity	Milestone 10C 5MM_Config script.pdf	Milestone 10 has 3 artifacts: 10 C) 5 Minute Meeting - [redacted] Configuration Script and onboarding [redacted]	66,062
Entity	Milestone 1 - [redacted]	Milestone 1 - Configuration Manuals fixed to include [redacted] component attributes.	295,910
Entity	Milestone 2 - [redacted]	Milestone 2 - [redacted] configuration manual Rev 0 from 2017.	304,640
Entity	Milestone 3 - [redacted]	Milestone 3 - EDRS Routing request demonstrating approval of the [redacted] Configuration Manual in 2017.	101,717

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 4 - [redacted].pdf	Milestone 4 - [redacted] to document an inventory of [redacted] in scope for NERC CIP.	190,698
Entity	Milestone 5 - [redacted].pdf	Milestone 5 - Updated [redacted] Document.	38,486
Entity	Milestone 6 - Training_Roster.pdf	Milestone 6 - A webex was held for the [redacted] administrators to train on the updated [redacted] document. Training Roster is attached.	408,170
Entity	Milestone 7 - TD-1210P-01-F01 Approval.docx	Milestone 7 - Approval of [redacted] in the EDRS System (Enterprise Document Routing System).	71,207

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.)

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

Attachment 2

2d. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R2 dated January 24, 2019

From: noreply@oati.net
Sent: 01/24/2019 14:02:29
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-1 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: WECC2018019480
Standard/Requirement: CIP-007-1 R2.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 11/09/2018 for the violation of CIP-007-1 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 3

3a. The Entity's Self-Report of violation of CIP-007-1 R3 submitted June 30, 2017

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-1

Requirement: CIP-007-1 R3.

Date Submitted: June 30, 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 22, 2009

End/Expected End Date: September 01, 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: Certain [redacted] include [redacted]
[redacted]
The [redacted] may be provided on a [redacted], or [redacted] [redacted] overlooked the [redacted] components when evaluating and applying firmware updates, so [redacted] did not evaluate and apply firmware updates on the [redacted] deployed as part of the [redacted] at [redacted] NERC high and medium impact sites. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines.

[redacted] will be submitting additional self-reports applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-007-1 R5, CIP-007-1 R6, CIP-010-2 R1 and CIP-010-2 R2 .

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Implementation of a patch/firmware update test on a sub-set of NERC CIP applicable [redacted] was completed on 10/30/2016. Firmware updates on all NERC CIP applicable [redacted] is scheduled to be completed on 9/1/2017.

Self Report

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: Unauthorized access to [redacted] could result in a loss of [redacted] This includes the [redacted] There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

Risk Assessment of Impact to BPS: Minimal as [redacted] would be promptly notified of the [redacted] from unauthorized access and restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 3

3b. The Entity's Mitigation Plan designated as WECCMIT013254-2 for CIP-007-1 R3 submitted August 9, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 3

NERC Violation ID	Requirement	Violation Validated On
WECC2017017880	CIP-007-1 R3.	03/01/2018

Mitigation Plan Submitted On: August 09, 2018

Mitigation Plan Accepted On: August 09, 2018

Mitigation Plan Proposed Completion Date: August 17, 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		
WECC2017017880	07/22/2009	CIP-007-1 R3.
Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).		

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

By routine monitoring of NERC CIP controls it was determined that [redacted] were not receiving firmware updates to mitigate known security vulnerabilities. This was discovered when the [redacted] were investigated for possible NERC CIP compliance gaps. The [redacted] are on a [redacted] When evaluating [redacted] during vulnerability management activities, [redacted] overlooked the [redacted] so [redacted] did not document vulnerabilities based on published vulnerabilities and current firmware versions.

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

As a result of analyzing published vulnerabilities and current firmware versions a list of was created that showed which [redacted] required firmware updates.

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. Create and test script to update firmware versions to prepare for 2017 spring patch cycle.
2. The approved firmware was uploaded to the [redacted] during the 2017 spring patch cycle.
3. Update [redacted] Cyber Assets [redacted] to include [redacted]
4. Provide Training on Vulnerability Management Program and [redacted] process
5. Revise Security Patch Management Procedure [redacted]

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: August 17, 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
Milestone 1 - Create and Test Script	Create and Test script to update firmware versions for 2017 spring patch cycle	10/02/2017	09/05/2017	Evidence of completion contained attached [redacted]	No
Milestone 2 - Firmware was uploaded to the [redacted]	Firmware updates applied to the [redacted] during the 2017 spring patch cycle	10/02/2017	09/05/2017	Evidence of completion contained attached documents [redacted]	No
Milestone 3 - Update [redacted] Cyber Assets [redacted]	Update [redacted] Cyber Assets On-boarding [redacted] to include [redacted]	10/02/2017	07/05/2017		No
Milestone 4 - Training on Vulnerability Management Program and [redacted] process	The training content covered the Vulnerability Management Program and [redacted] process prior to go live on January 2nd 2018. [redacted] has implemented a new vulnerability and security patch management solution call [redacted] to receive,	12/14/2017	12/14/2017		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
	correlate, prioritize, and track alerts. The [redacted] solution utilizes a risk-based and real-time approach for prioritizing remediation to help focus your efforts on high risk.				
Milestone 4a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	03/14/2018	03/14/2018		No
Milestone 4b - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	06/14/2018	06/14/2018		No
Milestone 5 - Revise the Security Patch Management Procedure [redacted]	Revise Security Patch Management Procedure [redacted] to include [redacted]	07/31/2018	07/06/2018		No

Additional Relevant Information

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.

Minimal Risk to BPS. Unauthorized access to [redacted] could result in a [redacted] This includes the [redacted]. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

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

[redacted] firmware updates will be included in future patch cycles as required. [redacted] are now included in the enterprise security vulnerability reporting and evaluation procedures that will prevent or minimize the probability of future violations.

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

[redacted] have been incorporated into the enterprise security vulnerability planning processes and procedures. A system matter expert has been identified who will be evaluating all future [redacted] related security vulnerability alerts.

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: June 30, 2017

Attachment 3

3c. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R3 submitted October 30, 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): WECC2017017880
Mitigated Standard Requirement(s): CIP-007-1 R3.
Scheduled Completion as per Accepted Mitigation Plan: August 17, 2018
Date Mitigation Plan completed: July 06, 2018
WECC Notified of Completion on Date: October 30, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 - EMS Patching [redacted].pdf	Milestones 1 & 2 - Change Request to complete Milestones 1 & 2 to update frimware for [redacted] associated with EMS	57,259
Entity	Milestone 1 - RAS Patching [redacted].pdf	Milestones 1 & 2 - Change Request to complete Milestones 1 & 2 to update frimware for [redacted] associated with RAS	68,330
Entity	Milestones 1 and 2 - IT Patching [redacted].pdf	Milestones 1 & 2 - Change Request to complete Milestones 1 & 2 to update frimware for [redacted] associated with IT systems	41,075
Entity	Milestones 1 and 2 - SCADA Patching [redacted].pdf	Milestones 1 & 2 - Change Request to complete Milestones 1 & 2 to update frimware for [redacted] associated with SCADA	61,433
Entity	Milestones 1 and 2 - ODS Patching [redacted].pdf	Milestones 1 & 2 - Change Request to complete Milestones 1 & 2 to update frimware for [redacted] associated with ODS	58,637
Entity	Milestone 2 - [redacted] Patch plan for [redacted].pdf	Milestone 2 - [redacted] Security Patch Mitigation Plan	259,220
Entity	Milestone 3 [redacted]	Milestone 3 - Updated [redacted] Cyber Assets [redacted] which includes [redacted]	188,496
Entity	Milestone 5 - [redacted]	Milestone 5 - Revised procedure [redacted] (Security Patch Management)	356,344
Entity	Milestone 5 - [redacted] report_[redacted].pdf	This file lists the vulnerabilities managed in 2017 and some current vulnerabilities. The file also contains a	428,396

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 5 - [redacted] report_[redacted].pdf	5 Minute Meeting presentation introducing [redacted].	428,396
Entity	Milestone 4 - Training Schedule_Roster - [redacted]	Milestone 4 - Training Schedule and Roster	16,892
Entity	CIP-007-1 R3 MP - Supplemental Narrative.pdf	supplemental narrative with screenshots to demonstrate how [redacted] related patches are identified and evaluated in [redacted] system and process. This document is to answer the WECC question: "We are missing evidence that the [redacted] tickets mention or require [redacted] to be evaluated for "patching" or firmware updates. Do any of the documents attached require this? Please let me know where that is in any processes or if we are missing a process document?"	923,184

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

3d. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R3 dated October 31, 2018

From: noreply@oati.net
Sent:
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-1 R3. - [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: WECC2017017880
Standard/Requirement: CIP-007-1 R3.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 10/30/2018 for the violation of CIP-007-1 R3.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

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

Attachment 4

4a. The Entity's Self-Report of violation of CIP-007-1 R5 submitted June 30, 2017

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-1

Requirement: CIP-007-1 R5.

Date Submitted: June 30, 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 22, 2009

End/Expected End Date: December 31, 2016

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

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: Certain [redacted] include [redacted] The [redacted] may be provided on a [redacted]. [redacted] overlooked the [redacted] and did not change the default passwords on the [redacted] deployed as part of the [redacted] at [redacted] NERC high and medium impact sites. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines.

[redacted] will be submitting additional self-reports applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-007-1 R3, CIP-007-1 R6, CIP-010-2 R1 and CIP-010-2 R2 .

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: All passwords were revised to utilize a shared administrator password while implementing Active Directory.

Self Report

Have Mitigating Activities been Completed? Yes

Date Mitigating Activities Completed: December 31, 2016

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Unauthorized access to [redacted] could result in a [redacted] This includes the [redacted]. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

Risk Assessment of Impact to BPS: Minimal as [redacted] would be promptly notified of the loss of server functionality from unauthorized access and restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 4

4b. The Entity's Mitigation Plan designated as WECCMIT013366-1 for CIP-007-1 R5 submitted August 9, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code:

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017017881	CIP-007-1 R5.	03/08/2018

Mitigation Plan Submitted On: August 09, 2018

Mitigation Plan Accepted On: August 09, 2018

Mitigation Plan Proposed Completion Date: October 05, 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		
WECC2017017881	07/22/2009	CIP-007-1 R5.
Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.		

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

By routine monitoring of NERC CIP controls it was established that default passwords were not changed as required for [redacted] The [redacted] are on a [redacted], or [redacted]. [redacted] overlooked the [redacted] so [redacted] did not recognize as requiring the application of the CIP standards.

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

As a result of interviews with subject matter experts, system administrators and [redacted] NERC CIP compliance analysts it was confirmed [redacted] did not meet CIP-007 R5 requirements.

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. Identify in-scope [redacted]
2. Create and test script to run on all [redacted] to update shared admin password.
3. Run Script on all in-scope [redacted]
4. Update [redacted] Cyber Assets [redacted] to include [redacted]
5. Train personnel on [redacted] Cyber Assets [redacted]
6. Update to [redacted] CIP-007 System Access Controls Procedure [redacted])
7. Develop a user guide to supplement the [redacted] procedure steps with job instructions related to [redacted]
8. Train personnel on revised procedure [redacted] and user guide.

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: October 05, 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
Milestone 1 - Identify in -scope [redacted]	List [redacted] that are in-scope for CIP-007 R5 mitigation plan.	11/04/2016	11/04/2016		No
Milestone 2 - Create and test script to run on all [redacted] to update shared admin password.	Create and test script to change admin passwords. Script contained a subroutine to confirm and report that the PW were successfully updated.	11/04/2016	11/04/2016		No
Milestone 3 - Run Script on all in-scope [redacted]	Create tickets to run script. Review data from results of script to verify script ran and PW's were updated.	11/04/2016	11/04/2016		No
Milestone 3a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	02/03/2017	02/03/2017		No
Milestone 3b - Schedule Correction	Adding Sub-milestone due to	05/05/2017	05/05/2017		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
	limitation of milestone completion dates in WebCDMS				
Milestone 4 - Update [redacted] Cyber Assets [redacted]	Update [redacted] Cyber Assets On-boarding [redacted] to include [redacted]	07/05/2017	07/05/2017		No
Milestone 4a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	10/05/2017	10/05/2017		No
Milestone 4b - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	01/05/2018	01/05/2018		No
Milestone 4c - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	04/06/2018	04/06/2018		No
Milestone 5 - Train personnel on new [redacted]	Provide training on [redacted] which is the [redacted] Cyber Assets [redacted] that includes [redacted]	05/29/2018	05/29/2018		No
Milestone 6 - Publish a new version of Revise [redacted] CIP-007 System Access Controls	Revise [redacted] to more clearly illustrate activities affecting [redacted] and the system access controls.	08/03/2018	05/31/2018		No
Milestone 7 - Develop User Guide for [redacted]	Develop a user guide to supplement the [redacted] procedure steps with job instructions related to [redacted]	08/31/2018			No
Milestone 8 - Train	Train impacted	09/28/2018			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
personnel on revised procedure [redacted]	personnel on the revised procedure [redacted] and user guide				

Additional Relevant Information

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.

Minimal - the [redacted] are within Physical and Electronic Security Perimeters with limited access. [redacted] has implemented defense-in-depth technical controls as well as Physical and Administrative controls to limit access to the [redacted]

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

By using enterprise change management systems for notification to change the passwords and only allowing a small select group of [redacted] personnel access to the [redacted] this will prevent or minimize the probability of future violations.

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: June 30, 2017

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

Attachment 4

4c. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R5 submitted October 5, 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): WECC2017017881
Mitigated Standard Requirement(s): CIP-007-1 R5.
Scheduled Completion as per Accepted Mitigation Plan: October 05, 2018
Date Mitigation Plan completed: October 04, 2018
WECC Notified of Completion on Date: October 05, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 [redacted] listing for CIP-007 R5 MP.pdf	Milestone 1 - List of [redacted] that are in-scope for CIP-007 R5 mitigation plan.	184,595
Entity	Milestone 2 evidence-email.pdf	Milestone 2 - email confirming script complete and ready to use	88,738
Entity	Milestone 3 _ [redacted]	Milestone 3 - Change request for password updates	45,807
Entity	Milestone 3 _ [redacted]	Milestone 3 - Change request for password updates	45,000
Entity	Milestone 3 _ [redacted]	Milestone 3 - Change request for password updates	50,587
Entity	Milestone 3 [redacted]	Milestone 3 - Change request for password updates	42,368
Entity	Milestone 3 _ [redacted]	Milestone 3 - Change request for password updates	42,161
Entity	[redacted]	Milestone 3 - Work order for password updates	32,939
Entity	Milestone 5 - [redacted]	Milestone 5 - [redacted] Training Roster	12,998
Entity	Milestone 4 - [redacted]	Milestone 4 - Updated [redacted] Cyber Assets [redacted]	188,500
Entity	Milestone 6 - [redacted]	Milestone 6 - Revised [redacted] to more clearly illustrate activities affecting LOMS [redacted] and the system access controls.	107,504

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 - Additional [redacted] Information.pdf	Milestone 1 - Additional [redacted] Information	284,654
Entity	Milestone 7 - Managing Shared User Accounts for [redacted] pdf	Milestone 7 - User guide to supplement the [redacted] procedure steps with job instructions related to [redacted] ([redacted]	208,280
Entity	Milestone 8 -Training.pdf	Training agenda for ODN CAB webex. Users were trained on account management procedure ([redacted]) and a new user guide for managed [redacted] shared accounts.	750,710
Entity	Milestone 8 - NERC training Roster 10042018.xlsx	This document is the training roster output from the Webex meeting. Personnel trained included [redacted] administrators and cyber system owners/SMEs.	21,096

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.)

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

Attachment 4

4d. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R5 dated January 18, 2019

From: noreply@oati.net
Sent:
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-1 R5. - [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: WECC2017017881
Standard/Requirement: CIP-007-1 R5.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 10/05/2018 for the violation of CIP-007-1 R5.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

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

Attachment 5

5a. The Entity's Self-Report of violation of CIP-007-1 R6 submitted June 30, 2017

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-007-1

Requirement: CIP-007-1 R6.

Date Submitted: June 30, 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 22, 2009

End/Expected End Date: July 31, 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: Certain [redacted] include [redacted] a [redacted]. The [redacted] may be provided on a [redacted] [redacted] overlooked the [redacted] and did not perform event logging of successful and unsuccessful logins on the [redacted] deployed as part of the [redacted] at [redacted] NERC high and medium impact sites. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines.

[redacted] will be submitting additional self-reports applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-007-1 R3, CIP-007-1 R5, CIP-010-2 R1 and CIP-010-2 R2 .

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Implement a manually initated security event log monitoring via [redacted] on all NERC CIP applicable [redacted] to be completed by 7/31/2017. Implement a [redacted] inventory capability in [redacted] to enable automated security event log monitoring via [redacted] to be completed by 12/1/2017.

Self Report

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: Unauthorized access to [redacted] could result in a [redacted] This includes the [redacted]. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

Risk Assessment of Impact to BPS: Minimal as [redacted] would be promptly notified of the loss of server functionality from unauthorized access and restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

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

Attachment 5

5b. The Entity's Mitigation Plan designated as WECCMIT013255-1 for CIP-007-1 R6 submitted May 29, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: WECCMIT013255-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017017882	CIP-007-1 R6.	03/21/2018

Mitigation Plan Submitted On: May 29, 2018

Mitigation Plan Accepted On: June 07, 2018

Mitigation Plan Proposed Completion Date: October 05, 2018

Actual Completion Date of Mitigation Plan: October 04, 2018

Mitigation Plan Certified Complete by [redacted] On: October 05, 2018

Mitigation Plan Completion Verified by WECC On: January 18, 2019

Mitigation Plan Completed? (Yes/No): Yes

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		
WECC2017017882	07/22/2009	CIP-007-1 R6.
Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.		

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

By routine monitoring of NERC CIP controls it was determined that [redacted] were not sending security logs to the enterprise logging system. This was discovered when the [redacted] were investigated for possible NERC CIP compliance gaps. The [redacted] are on a [redacted]. When evaluating [redacted] during security log monitoring activities, [redacted] overlooked the [redacted] so [redacted] did not investigate possible compliance gaps for monitoring security logs.

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

All [redacted] versions in use were investigated to determine what versions were capable of recording and sending logs. Event logging of successful and unsuccessful logins was not performed on [redacted]

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. Create and test script to configure [redacted] to send logs to the enterprise logging system.
2. Run script on all [redacted] to modify configuration allowing logs to be sent to enterprise logging system
3. Utilize enterprise logging system, [redacted] to confirm successful and unsuccessful logs are being analyzed.
4. Update New Asset Onboarding [redacted]
5. Update [redacted] CIP-007 Security Event Monitoring Procedure [redacted]
6. Training and stakeholder awareness of updated [redacted] CIP-007 Security Event Monitoring Procedure [redacted] and Asset Onboarding [redacted]

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: October 05, 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
Milestone 4 - Update New Asset Onboarding [redacted]	The [redacted] specifically prescribes [redacted] be onboard to CIP-007 and CIP-010 systems and controls for CIP Cyber Assets	07/25/2017	07/25/2017		No
Milestone 1 - Create and Test Script to configure [redacted]	Create and test script to configure [redacted] to send logs to the enterprise logging system. Functional test script used across current hardware versions.	10/02/2017	05/31/2017	Evidence of completion contained in document DOC [redacted]	No
Milestone 2 - Run script on all [redacted] to modify configuration	Run script on al[redacted] [redacted] to modify configuration allowing logs to be sent to enterprise logging system.	10/02/2017	07/20/2017	Evidence of completion contained in document DOC [redacted]	No
Milestone 3 - Confirm	Utilize enterprise	10/02/2017	07/31/2017	Evidence of completion	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
log records from enterprise logging system	logging system, [redacted] to confirm successful and unsuccessful logs are being analyzed.			contained in documents DOC IDs [redacted]	
Milestone 4a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	10/25/2017	10/25/2017		No
Milestone 4b - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	01/25/2018	01/25/2018		No
Milestone 4c - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	04/25/2018	04/25/2018		No
Milestone 5 - Update [redacted] CIP-007 Security Event Monitoring Procedure [redacted]	Revision of CIP-007 procedure will include a specific note about applicability to lights-out or out-of-band management devices. This milestone may be completed before the proposed completion date.	07/25/2018	07/06/2018	Procedure updated on 7/6/2018.	No
Milestone 6 - Training of updated [redacted] CIP-007 Security Event Monitoring Procedure [redacted] & Asset [redacted]	Webex/Tailboard training of updated [redacted] CIP-007 Security Event Monitoring Procedure [redacted] and Asset [redacted]. This milestone may be completed before the proposed completion date.	08/31/2018	10/04/2018	Training was performed during the weekly [redacted] call. Training included milestones for CIP-007-1 R5 and R6 [redacted] Mitigation Plans). Training roster included applicable [redacted] administrators and Cyber System owners/SMEs. (See evidence for Milestone 6)	No

Additional Relevant Information

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.

Minimal - the [redacted] are within Physical and Electronic Security Perimeters with limited access. [redacted] has implemented defense-in-depth technical controls as well as Physical and Administrative controls to limit access to the [redacted] This issue had been remediated because [redacted] logs are now being sent to the enterprise logging system.

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

Logs will be sent to and analyzed by [redacted] the enterprise logging system upon completion of this mitigation plan. Procedure documents will be updated to include [redacted] Training and stakeholder awareness on updated processes will be completed by the conclusion of this mitigation plan.

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

[redacted] will be included in the enterprise asset inventory system to enable automated security monitoring by Q1 2018.

The onboarding procedure for [redacted] will be modified to include specific instructions for onboarding the [redacted] including how to verify that logs are analyzed. The onboarding procedure is scheduled to be updated and approved in Q4 of 2017.

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: [redacted]

Attachment 5

5c. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R6 submitted October 5, 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): WECC2017017882
Mitigated Standard Requirement(s): CIP-007-1 R6.
Scheduled Completion as per Accepted Mitigation Plan: October 05, 2018
Date Mitigation Plan completed: October 04, 2018
WECC Notified of Completion on Date: October 05, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 1 - WO 2751719 to test for [redacted] logging.pdf	Milestone 1 - Work Order (screen shot) to setup & test a [redacted] to send logs to [redacted]	23,771
Entity	Milestone 2 - [redacted].pdf	Milestone 2 - Change request to run script to configure [redacted] to log to [redacted]	34,233
Entity	Milestone 3 - Evidence of [redacted] logging.docx	Milestone 3 - Document showing [redacted] are being logged	43,126
Entity	Milestone 3 - [redacted] down ports to non-logging [redacted] docx	(Milestone 3) File showing [redacted] switch ports downed because the [redacted] on the ports were not licensed	443,675
Entity	Milestone 4 - [redacted]	Revised Asset Onboarding [redacted] TD-1210-F01 Rev 2.	188,500
Entity	Milestone 5 - [redacted]	Updated CIP-007 Security Event Monitoring Procedure [redacted]	91,453
Entity	Milestone 5 - [redacted]	[redacted] published a new version of [redacted] to strengthen language to support inclusion of [redacted] in the process (lights out management).	106,008
Entity	Milestone 6 - Training.pdf	Training was performed during the weekly ODN CAB call. Training included milestones for CIP-007-1 R5 and R6 ([redacted] Mitigation Plans).	687,479
Entity	Milestone 6 - NERC training Roster 10042018.xlsx	Training was performed during the weekly ODN CAB call. Training included milestones for CIP-007-1 R5 and R6 ([redacted] Mitigation Plans). Training Roster is an output from WEBEX that demonstrates all attendees on the call. Training audience include	21,096

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone 6 - NERC training Roster 10042018.xlsx	[redacted] admins and cyber system owners/SMEs who are responsible for [redacted] controls and documentation for CIP-007.	21,096

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.)

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

Attachment 5

5d. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R6 dated January 18, 2019

From: noreply@oati.net
Sent:
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-1 R6. - [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: WECC2017017882
Standard/Requirement: CIP-007-1 R6.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 10/05/2018 for the violation of CIP-007-1 R6.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 6

6a. The Entity's Self-Report of violation of CIP-007-1 R8 submitted April 3, 2018

Self Report

Entity Name [redacted]

NERC ID [redacted]

Standard: CIP-007-1

Requirement: CIP-007-1 R8.

Date Submitted: April 03, 2018

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 22, 2009

End/Expected End Date:

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

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] initially failed to develop a formal configuration manual that included details on the configuration attributes for [redacted] Additionally, [redacted] Cyber Asset [redacted] did not include checks or steps to account for the [redacted] of the physical server. This lack of configuration documentation and verification led to the [redacted] being overlooked during [redacted] enumeration of the physical [redacted] configurations.
This oversight and lack of configuration information for the physical server [redacted] also contributed to their exclusion from [redacted] Cyber Vulnerability Assessment port and services verification and default account review.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: [redacted] were included in the [redacted] 2017 Cyber Vulnerability Assessment which was completed on June 16, 2017.
[redacted] team developed a configuration manual in September 2017. That same team made revisions, in July 2017, to [redacted] to include [redacted] in order to facilitate the verification process. Both mitigation actions support the server component inclusion function of configuration and change

management.

Have Mitigating Activities been Completed? Yes

Date Mitigating Activities Completed: September 27, 2017

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Unauthorized access to [redacted] could result in a loss of [redacted]. This includes the [redacted]

Risk Assessment of Impact to BPS: There was minimal risk of unauthorized access because the [redacted] are located within [redacted] physical and Electronic Security Perimeters, and only a select group of [redacted] personnel had access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS because no unauthorized access occurred.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	[redacted] Manual approved 9/27/2017. Manual is in the process of being revised to correct format.	249,120
Entity	[redacted]	[redacted] Manual Approval document.	67,450
Entity	[redacted]	Updated [redacted] Cyber Assets [redacted] Update included [redacted] on [redacted]	188,495

Attachment 6

6b. The Entity's Mitigation Plan designated as WECCMIT014136 for CIP-007-1 R8 submitted September 18, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: WECCMIT014136

Mitigation Plan Version: 1

NERC Violation ID	Requirement	Violation Validated On
WECC2018019481	CIP-007-1 R8.	07/19/2018

Mitigation Plan Submitted On: September 18, 2018

Mitigation Plan Accepted On: September 26, 2018

Mitigation Plan Proposed Completion Date: October 19, 2018

Actual Completion Date of Mitigation Plan: October 12, 2018

Mitigation Plan Certified Complete by [redacted] On: October 16, 2018

Mitigation Plan Completion Verified by WECC On: January 24, 2019

Mitigation Plan Completed? (Yes/No): Yes

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		
WECC2018019481	07/22/2009	CIP-007-1 R8.
Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:		

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

[redacted] initially failed to develop a formal configuration manual that included details on the configuration attributes for [redacted] Additionally, [redacted] Cyber Asset [redacted] did not include checks or steps to account for the [redacted] component of the physical server. This lack of configuration documentation and verification led to the [redacted] being overlooked during [redacted] enumeration of the physical server configurations. This oversight and lack of configuration information for the physical server [redacted] component also contributed to their exclusion from [redacted] Cyber Vulnerability Assessment port and services verification and default account review.

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

WECC notified [redacted] of the violation after reviewing the other [redacted] Self Reports.

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:

The [redacted] were not originally identified as components of NERC CIP Cyber Assets prior to the reported condition and were therefore not captured in the CIP program's processes.

[redacted] has completed or will complete activities to ensure the remediation of this violation and prevention of recurrence of this violation.

Actions Completed Include:
Milestone 1: Update [redacted] baseline configurations to include all [redacted] Attributes.
Milestone 2: Perform the 2017 Vulnerability Assessment and include the [redacted] (Completed June 16, 2017).
Milestone 3: Update and Publish [redacted] configuration manual.
Milestone 4: Configure the [redacted] to display a listing of [redacted] The [redacted] will be displayed on the [redacted] tab of the [redacted] NERC Portal.
Milestone 5: Update and Publish [redacted]
Milestone 6: Update and Publish [redacted]
Milestone 7: Train [redacted] administrators on changes [redacted]
Milestone 8: Perform 2018 Vulnerability Assessment and ensure inclusion of [redacted] per procedure.

Actions Pending Include:
Milestone 9: Update and Publish [redacted]
Procedure to supplement the language for [redacted]

As a result of actions and milestones completed in this mitigation plan, [redacted] now maintains an inventory of enabled [redacted] in scope for NERC CIP and has a series of guidance documents that instruct personnel to apply protective security measures to the components and verify on a routine basis.

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: October 19, 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
Milestone 1: Update [redacted] Baseline Configurations	Update [redacted] baseline configurations to include all [redacted] Attributes.	03/31/2017	03/31/2017	This milestone is complete. In accordance with [redacted] Configuration Change Management, the [redacted] have been documented in a baseline configuration.	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
Milestone 2: Perform 2017 VA on [redacted]	Perform 2017 Vulnerability Assessment on [redacted]	06/16/2017	06/16/2017	[redacted] performed an Active and Paper Vulnerability Assessment (VA) on applicable cyber assets including the in scope [redacted] that were enabled in production at the time of the VA kickoff.	No
Milestone 2a	Time extension Placeholder	09/01/2017	09/01/2017		No
Milestone 3: Publish [redacted] Configuration Manual	Publish [redacted] Configuration Manual [redacted]	09/27/2017	09/27/2017	[redacted] has verified that the milestone is completed and the documentation is located in [redacted]	No
Milestone 3a	Time extension placeholder.	12/27/2017	12/27/2017		No
Milestone 4: Configure [redacted]	Configure the [redacted] to display a listing of [redacted] The [redacted] will be displayed on the [redacted] tab of the [redacted] NERC Portal.	02/01/2018	02/01/2018	Deployed in [redacted] release 5.0	No
Milestone 4a	Time extension placeholder	05/01/2018	05/01/2018		No
Milestone 5: Update VA Procedure and Publish	Update and Publish [redacted] Procedure to include language for [redacted]	05/09/2018	05/09/2018	Updated procedure revision includes specific language calling out the [redacted] as part of the VA scope.	No
Milestone 6: Update and Publish [redacted]	Update and Publish [redacted]	06/30/2018	07/31/2018	The [redacted] now calls out the associated [redacted] specific steps by name.	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
	[redacted]				
Milestone 7: Training	Perform training for administrator on [redacted]	07/03/2018	07/03/2018	All administrators have been trained and a log of the meeting was captured	No
Milestone 8: Perform 2018 VA	Perform 2018 VA in accordance with [redacted] and ensure inclusion of [redacted]	07/12/2018	07/12/2018	2018 VA was completed and included [redacted] per the procedure scope.	No
Milestone 9: Publish updated VA Procedure	Update and Publish [redacted] Procedure to supplement the language for [redacted] The Annual VA section of the procedure so the [redacted] are clearly called out in both the Ad hoc VA section (CIP-010-2 R3.3) and the annual VA section (CIP-010-2 R3.1/3.2).	10/12/2018	09/19/2018	The procedure already includes [redacted] language but this will enhance procedural steps and language to incorporate [redacted] and other components in the annual VA section. 9/14 - revised Milestone description to clarify how this milestone differs from milestone 5. Evaluation discovered that the procedure required additional updates beyond milestone 5. 9/19 - Document revised and published.	No

Additional Relevant Information

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.

(i) Minimal Risk - Unauthorized access to [redacted] could result in a [redacted] This includes the [redacted] are in place to reduce risk.
(ii) The [redacted] were assessed through the annual vulnerability assessment in both 2017 and 2018. [redacted] are now included in the NERC CIP [redacted] and related VA procedure [redacted] dictates performing the assessment on [redacted] components. Therefore, this violation and the risk to the lack of control over the VA has been remediated since June 2017.

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

[redacted] follows the [redacted] procedure to develop test plans and assess in scope assets and components which include the [redacted]
As a result of actions and milestones completed in this mitigation plan, [redacted] now maintains an inventory of enabled [redacted] in scope for NERC CIP and has a series of guidance documents that instruct personnel to apply protective security measures to the components and verify on a routine basis. Guidance documents include administrative and technical controls to prevent, detect and correct configuration issues with the [redacted] components.

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

Part of the [redacted] procedure is to conduct a lessons learned meeting for continuous improvement. The purpose is to identify opportunities for improvement and improve process and testing for the next instance of the VA.

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: [redacted]

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

Attachment 6

6c. The Entity's Certification of Mitigation Plan Completion for CIP-007-1 R8 submitted October 16, 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): WECC2018019481

Mitigated Standard Requirement(s): CIP-007-1 R8.

Scheduled Completion as per Accepted Mitigation Plan: October 19, 2018

Date Mitigation Plan completed: October 08, 2018

WECC Notified of Completion on Date: October 16, 2018

Entity Comment: Milestone 3 evidence was updated with a revised procedure published on 10/8/18.

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	C7R8MP_MS1_baseline config_include _[redacted]Attributes.pdf	Milestone 1: Evidence that configuration baselines include [redacted] components.	295,910
Entity	C7R8MP_MS2_2017_VA_Final_Report.pdf	Milestone 2: See 'Background and Scope' on Page 2 and 'Assessment Results' on Page 4. [redacted] were included in the scope of the 2017 annual VA.	613,839
Entity	C7R8MP_MS5_TD_1210P_03.pdf	Milestone 5: VA Procedure with [redacted] language added.	225,136
Entity	C7R8MP_MS6_1210P_01_F01.pdf	Milestone 6: TD-1210P-01-F01 Updated to include [redacted] steps.	38,486
Entity	C7R8MP_MS7_5MM_training_Roster.pdf	Milestone 7: Webex training attendance roster for a meeting that briefed a 5 minute meeting on the updated [redacted] from Milestone 6. Attendance included [redacted] administrators	406,972
Entity	C7R8MP_MS4_ [redacted]AMP.pdf	Milestone 4: The [redacted] NERC CIP Asset Management System now contains a tab for [redacted] ([redacted]).	190,698
Entity	C7R8MP_MS3_[redacted]CM.pdf	Milestone 3: [redacted] Configuration Manual was created in 2017. [redacted] updated the document in 2018 and published revision 2.0 in October to improve the document (Rev 2.0 attached). Rev 1 was provided in other [redacted] related self reports to WECC in 2017.	578,120
Entity	C7R8MP_MS8_2018_VA_DRAC_Test_Plan.pdf	Milestone 8: Attachment is a pdf copy of the VA test plan spreadsheet for the [redacted] devices testing	1,025,776

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	C7R8MP_MS8_2018_VA_DRAC_Test_Plan.pdf	Logical Ports.	1,025,776
Entity	C7R8MP_MS9_RevTD_1210P_03.pdf	Milestone 9: Updated version of TD-1210P-03 with more instructions to call out [redacted] in the annual VA section.	259,623

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.)

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

Attachment 6

6d. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R8 dated January 24, 2019

From: noreply@oati.net
Sent: 01/24/2019 1[redacted]19:58
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-007-1 R8. - [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: WECC2018019481
Standard/Requirement: CIP-007-1 R8.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 10/16/2018 for the violation of CIP-007-1 R8.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 7

7a. The Entity's Self-Report of violation of CIP-010-2 R1 submitted June 30, 2017

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-010-2

Requirement: CIP-010-2 R1.

Date Submitted: June 30, 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: March 31, 2017

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

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: Certain CIP-002 inventoried [redacted] include [redacted] a [redacted]. The [redacted] When preparing the baseline configuration for [redacted], [redacted] overlooked the [redacted] so [redacted] did not document the [redacted] in the baseline configurations. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines.

[redacted] will be submitting additional self-reports applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-007-1 R3, CIP-007-1 R5, CIP-007-1 R6 and CIP-010-2 R2 .

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Added all the [redacted] attributes to [redacted] Baselines by 3/31/2017. Added all the [redacted] attributes to [redacted] Baselines by 3/31/2017.

Self Report

Have Mitigating Activities been Completed? Yes

Date Mitigating Activities Completed: March 31, 2017

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Unauthorized access to [redacted] could result in a loss of [redacted] This includes the [redacted] There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

Risk Assessment of Impact to BPS: Minimal as [redacted] would be promptly notified of the loss of server functionality from unauthorized access and restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 7

7b. The Entity's Mitigation Plan designated as WECCMIT013348-1 for CIP-010-2 R1 submitted June 25, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity: [redacted]

Mitigation Plan Code: WECCMIT013348-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017017883	CIP-010-2 R1.	04/02/2018

Mitigation Plan Submitted On: June 25, 2018

Mitigation Plan Accepted On: June 25, 2018

Mitigation Plan Proposed Completion Date: August 01, 2018

Actual Completion Date of Mitigation Plan: June 29, 2018

Mitigation Plan Certified Complete by [redacted] On: July 31, 2018

Mitigation Plan Completion Verified by WECC On: September 14, 2018

Mitigation Plan Completed? (Yes/No): Yes

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		
WECC2017017883	07/01/2016	CIP-010-2 R1.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.		

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

Certain CIP-002 inventoried [redacted] include [redacted] a [redacted]. The [redacted] When preparing the baseline configuration for [redacted], [redacted] overlooked the [redacted], so [redacted] did not document the [redacted] in the baseline configurations. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines. [redacted] has submitted an additional self-report and mitigation plan applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-010-2 R2.

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

During routine sampling of IT assets for compliance requirements and interviews with systems administrators.

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. Update [redacted] Baseline Configurations to include all [redacted] attributes.
2. Update New Asset Onboarding [redacted]
3 Update to [redacted] CIP-010 Configuration Change Management Procedure [redacted]
4 Training and stakeholder awareness of updated [redacted] CIP-010 Configuration Change Management Procedure [redacted] and Asset Onboarding [redacted]
5. CIP-010-2 Web-based Training (WBT) Development

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: August 01, 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
Milestone 1 - Update [redacted] Server baseline configurations to include al[redacted] attributes.	Added all the [redacted] attributes to [redacted] Baselines.	04/14/2017	03/31/2017	[redacted] baselines requirements have been added to all baselines for [redacted]	No
Milestone 2 - Update New Asset Onboarding [redacted]	The [redacted] specifically prescribes [redacted] be onboard to CIP-007 and CIP-010 systems and controls for CIP Cyber Assets	07/05/2017	07/05/2017		No
Milestone 2a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	10/05/2017	10/05/2017		No
Milestone 2b - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	01/05/2018	01/05/2018		No
Milestone 2c - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion	04/05/2018	04/05/2018		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
	dates in WebCDMS				
Milestone 3 - Update to [redacted] CIP-010 Configuration Change Management Procedure	Revision of CIP-010 R1 procedure [redacted] will include a specific note about enumeration of lights-out or out-of-band management devices	05/18/2018	05/11/2018		No
Milestone 4 - Training of [redacted] CIP-010 Configuration Change Management Procedure [redacted] & [redacted]	WebEx and Tailboard Training of updated [redacted] CIP-010 Configuration Change Management Procedure [redacted] and [redacted] .	06/30/2018	06/18/2018		No
Milestone 5 - CIP-010-2 Web-based Training (WBT) Development	Develop WBT to review the [redacted] policies and procedures we maintain to ensure compliance with CIP-010 requirements to prevent and detect unauthorized changes to BES Cyber Systems. Topics include the development of baseline configuration for High or Medium Impact BCA, configuration change management and processes for vulnerability	07/23/2018	06/29/2018		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
	assessments. A web-based training (WBT) including interactive content and knowledge checks will be used to cover the topics in this course. Completion of the WBT will be required annually and included in employee's training curriculum starting in 2019.				

Additional Relevant Information

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.

Minimal risk to BPS. Unauthorized access to [redacted] could result in a [redacted]. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred. This issue has been remediated because [redacted] now have a baseline configuration.

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

Detection of configuration changes will be discovered and addressed expeditiously by using advertised automated and manual processes that will prevent or minimize the probability of future violations. Procedural documents have been updated to in [redacted] Training and stakeholder awareness on updated processes will be completed by the conclusion of this mitigation plan.

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

All unauthorized changes that are discovered will be recorded and tracked to completion using the existing enterprise work tracking system for CIP-010 R2 tracking and remediation.

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: [redacted]

Attachment 7

7c. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R1 submitted July 31, 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): WECC2017017883
Mitigated Standard Requirement(s): CIP-010-2 R1.
Scheduled Completion as per Accepted Mitigation Plan: August 01, 2018
Date Mitigation Plan completed: July 31, 2018
WECC Notified of Completion on Date: July 31, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Milestone [redacted]	Milestone 1 Snapshot of [redacted] Document Routing System showing completion of the [redacted] being integrated into the baselines..	69,916
Entity	Milestone 1_[redacted]	Milestone 1 - [redacted] server baseline file identified in snapshot	116,315
Entity	Milestone 1 _[redacted]	Milestone 1 - [redacted] server baseline file identified in snapshot	117,239
Entity	Milestone 1_[redacted]	Milestone 1 - [redacted] server baseline file identified in snapshot	114,684
Entity	[redacted]	Milestone 2 - Updated [redacted] Cyber Assets [redacted] which includes [redacted]	188,496
Entity	Milestone 3 _[redacted]	[redacted] CIP-010 Configuration Change Management Procedure TD-1210P-01 Rev 4	352,797
Entity	Milestone 4 -[redacted]	CIP-010 R1 & R2 Training Roster	13,635
Entity	Milestone 5 -[redacted]	Milestone 5 - Executive Summary of completed Web Based Training (WBT) curriculum. (See highlighted area on page 3 for the CIP-010 WBT)	505,603

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.)

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

Attachment 7

7d. WECC's Verification of Mitigation Plan Completion for CIP-010-2 R1 dated September 14, 2018

From: noreply@oati.net
Sent:
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 R1. - [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: WECC2017017883
Standard/Requirement: CIP-010-2 R1.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 07/31/2018 for the violation of CIP-010-2 R1.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]

Attachment 8

8a. The Entity's Self-Report of violation of CIP-010-2 R2 submitted June 30, 2017

Self Report

Entity Name: [redacted]

NERC ID: [redacted]

Standard: CIP-010-2

Requirement: CIP-010-2 R2.

Date Submitted: June 30, 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: June 29, 2017

Reliability Functions: [redacted]

Is Possible Violation still occurring?: No

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: Certain CIP-002 inventoried [redacted] include [redacted] e. The [redacted] may be provided on a [redacted] or [redacted]. When preparing the baseline configuration for [redacted], [redacted] overlooked the [redacted] so [redacted] did not document the [redacted] s in the baseline configurations. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance [redacted] began corrective action to include the [redacted] in the baselines.

[redacted] will be submitting additional self-reports applicable to [redacted] at NERC high and medium impact sites for NERC requirements CIP-007-1 R3, CIP-007-1 R5, CIP-007-1 R6 and CIP-010-2 R1 .

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: 1. Implemented an automated [redacted] configuration monitoring system in [redacted] Completed on 5/31/2017.
2. Implemented a manual monitoring process for systems unable to be monitored in [redacted] Completed on 6/29/2017.

Self Report

3. Troubleshoot and enable 90% or more automated monitoring in [redacted] Scheduled to be completed by 7/31/2017.

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: Unauthorized access to [redacted] could result in a loss of server functionality (e.g., [redacted]). This includes the [redacted]. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred.

Risk Assessment of Impact to BPS: Minimal as [redacted] would be promptly notified of the loss of server functionality from unauthorized access and restore access.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 8

8b. The Entity's Mitigation Plan designated as WECCMIT013256-1 for CIP-010-2 R2 submitted August 9, 2018

Mitigation Plan

Mitigation Plan Summary

Registered Entity [redacted]

Mitigation Plan Code: WECCMIT013256-1

Mitigation Plan Version: 2

NERC Violation ID	Requirement	Violation Validated On
WECC2017017884	CIP-010-2 R2.	04/02/2018

Mitigation Plan Submitted On: August 09, 2018

Mitigation Plan Accepted On: August 09, 2018

Mitigation Plan Proposed Completion Date: August 15, 2018

Actual Completion Date of Mitigation Plan: June 29, 2018

Mitigation Plan Certified Complete by [redacted] On: August 13, 2018

Mitigation Plan Completion Verified by WECC On: September 18, 2018

Mitigation Plan Completed? (Yes/No): Yes

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		
WECC2017017884	08/05/2016	CIP-010-2 R2.
Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring.		

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

Certain CIP-002 inventoried [redacted] include [redacted] that allows for monitoring and management of the [redacted]. The [redacted] may be provided on a [redacted] When preparing the baseline configuration for [redacted] overlooked the [redacted] subcomponents, so [redacted] did not document the [redacted] in the baseline configurations. [redacted] became aware of this last year and asked for guidance from the WECC. Upon receiving guidance, [redacted] began corrective action to include the [redacted] in the baselines. [redacted] has submitted additional self-report and mitigation plan applicable to [redacted] at NERC high and medium impact sites for NERC requirements in CIP-010-2 R1.

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

No additional information

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. Automate [redacted] configuration monitoring in [redacted] There are [redacted] Associated with BES Facilities.
2. Implement manual monitoring process for systems unable to monitor in [redacted]
3. Troubleshoot and enable 90% or more automated monitoring in [redacted]
4. Update Asset [redacted]
5. Update [redacted] CIP-010 Configuration Monitoring Procedure [redacted]
6. Training and stakeholder awareness of updated [redacted] CIP-010 Configuration Monitoring Procedure [redacted] and Asset [redacted]
7. CIP-010-2 Web-based Training (WBT) Development

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: August 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
Milestone 4 - Update Asset Onboarding [redacted]	The [redacted] specifically prescribes [redacted] be onboard to CIP-007 and CIP-010 systems and controls for CIP Cyber Assets	07/25/2017	07/05/2017		No
Milestone 1 - Automate [redacted] configuration monitoring in [redacted]	Automated monitoring of configuration of [redacted] There are [redacted] High Impact [redacted] Associated with BES Facilities.	10/02/2017	05/31/2017	Evidence of completion contained in attached documents DOC IDs [redacted]	No
Milestone 2 - Implement manual monitoring process for systems unable to monitor in [redacted]	Created process for monitoring configuration for [redacted] outside of the automation process.	10/02/2017	06/29/2017	Evidence of completion contained in attached document DOC ID [redacted]	No
Milestone 3 -	Enabled more than	10/02/2017	06/30/2017	Evidence of completion	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
Troubleshoot and enable 90% or more automated monitoring in [redacted]	90% to be monitored by automation.			contained in attached documents DOC IDs [redacted]	
Milestone 4a - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	10/25/2017	10/25/2017		No
Milestone 4b - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	01/25/2018	01/25/2018		No
Milestone 4c - Schedule Correction	Adding Sub-milestone due to limitation of milestone completion dates in WebCDMS	04/25/2018	04/25/2018		No
Milestone 5 - Update to [redacted] CIP-010 Configuration Monitoring Procedure [redacted]	Revision of CIP-010 R2 procedure will include a specific note about applicability to lights-out or out-of-band management devices	06/30/2018	06/22/2018		No
Milestone 6 - Training of updated Configuration Monitoring Procedure [redacted] and [redacted]	WebEx and Tailboard training of updated [redacted] CIP-010 Configuration Monitoring Procedure [redacted] and [redacted]	06/30/2018	06/18/2018		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
	.				
Milestone 7 - CIP-010-2 Web-based Training (WBT) Development	Develop WBT to review the [redacted] policies and procedures we maintain to ensure compliance with CIP-010 requirements to prevent and detect unauthorized changes to BES Cyber Systems. Topics include the development of baseline configuration for High or Medium Impact BCA, configuration change management and processes for vulnerability assessments. A web-based training (WBT) including interactive content and knowledge checks will be used to cover the topics in this course. Completion of the WBT will be required annually and included in affecting employee's training curriculum starting in 2019.	07/23/2018	06/29/2018		No

Additional Relevant Information

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.

Minimal Risk to BPS. Unauthorized access to [redacted] could [redacted]. This includes the [redacted] systems. There was minimal risk of unauthorized access as the [redacted] are located within [redacted] Physical and Electronic Security Perimeters, and only a select group of [redacted] personnel could have access - authorized or unauthorized - to the [redacted] There was no actual impact to the BPS as no unauthorized access occurred. [redacted] monitoring of the baselines has been remediated. Manual and automated processes have been created for baseline monitoring.

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

Detection of configuration changes will be discovered and addressed expeditiously by using advertised automated and manual processes that will prevent or minimize the probability of future violations. Processes have been updated to include [redacted] Training and stakeholder awareness on updated processes will be completed by the conclusion of this mitigation plan.

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

Configurations baselines will be maintained in accordance with CIP-010 R1 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: [redacted]

Attachment 8

8c. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted August 13, 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): WECC2017017884
Mitigated Standard Requirement(s): CIP-010-2 R2.
Scheduled Completion as per Accepted Mitigation Plan: August 15, 2018
Date Mitigation Plan completed: June 29, 2018
WECC Notified of Completion on Date: August 13, 2018
Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	Mileston 1 and 3 [redacted]	(Milestones 1 & 3) Output file from [redacted] that shows ports and services.	112,260
Entity	Milestones 1 and 3 - [redacted]	(Milestones 1 & 3) Output file from [redacted] that shows firmware versions.	18,579
Entity	Milestone 2 TD-1210P-02-JA01_v0.pdf	(Milestone 2) Job Aid that details steps needed for manual monitoring of [redacted]	67,304
Entity	Milestone 3 - [redacted]	(Milestone 3) Review of Baseline for June 2017	31,741
Entity	Milestone 3 - [redacted]	(Milestone 3) Screen shots from [redacted] that show [redacted] disabled after discovering port [redacted] was active and not an approved port.	249,545
Entity	Milestone 4 - [redacted]	Milestone 4 - TD-1210-01-F01 Rev2 [redacted] Onboarding [redacted]	188,500
Entity	Milestone 5 - [redacted]	Milestone 5 - TD-1210P-02 Rev 4 (CIP-010 Configuration Monitoring Procedure)	194,526
Entity	Milestone 6 - [redacted]	Milestone 6 - CIP-010 R1 and R2 Training Roster	13,638
Entity	Milestone 7 - Executive Summary of Developed Web	Milestone 7 - Executive Summary of completed Web Based Training (WBT) curriculum. (See highlighted	505,603

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[redacted]	area on page 3 for the CIP-010 WBT)	505,603

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.)

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

Attachment 8

8d. WECC's Verification of Mitigation Plan Completion for CIP-010-2 R2 dated September 18, 2018

From: noreply@oati.net
Sent: 09/18/2018 08:52:38
To: [redacted]
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 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: WECC2017017884
Standard/Requirement: CIP-010-2 R2.
Subject: Completed Mitigation Plan Acceptance

The Western Electricity Coordinating Council (WECC) received the Certification of Mitigation Plan Completion submitted by [redacted] on 08/13/2018 for the violation of CIP-010-2 R2.. After a thorough review, WECC has accepted the Certification of Mitigation Plan Completion.

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

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

[OATI Information - Email Template: MitPlan_Completed]