

October 31, 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. NP20-\_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty<sup>1</sup> regarding noncompliance by [REDACTED] (referred to herein as The Entity), NERC Registry ID# [REDACTED]<sup>2</sup> with information and details regarding the nature and resolution of the violations<sup>3</sup> 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)).<sup>4</sup>

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and The Entity have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of the CIP Reliability Standards listed below.

---

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

<sup>2</sup> [REDACTED]

<sup>3</sup> 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.

<sup>4</sup> See 18 C.F.R. § 39.7(c)(2) and 18 C.F.R. § 39.7(d).

1325 G Street NW Suite 600  
Washington, DC 20005  
202-400-3000 | [www.nerc.com](http://www.nerc.com)

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 2

According to the Settlement Agreement, The Entity admits to the violations and has agreed to the assessed penalty of three hundred seventy-eight thousand dollars (\$378,000), 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, 18 C.F.R. § 39.7 (2019), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement and herein.

NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method*	Violation Start-End Date	Risk	Penalty Amount
WECC2018019376	CIP-007-6	R5	Medium/Severe	█	CA 2/26/2018-3/2/2018	7/1/2016-5/10/2018	Minimal	\$378k
WECC2018019192	CIP-010-2	R1	Medium/Severe	█	SR 2/13/2018	7/1/2016-11/20/2018	Serious	
WECC2017018484	CIP-010-2	R1	Medium/Severe	█	SR 10/12/2017	7/1/2016-6/1/2017	Moderate	
WECC2017018485	CIP-010-2	R2	Medium/Severe	█	SR 10/12/2017	7/25/2017-8/15/2017; 8/5/2016-6/1/2017	Moderate	
WECC2018019012	CIP-010-2	R2	Medium/Severe	█	SR 1/19/2018	3/14/2017-1/16/2018	Moderate	

FACTS COMMON TO VIOLATIONS

NERC Notice of Penalty

The Entity

October 31, 2019

Page 3



The Entity violated the CIP Reliability Standards when it failed to develop baseline configurations for its Bulk Electric System Cyber Assets and to test changes to those configurations before deploying them in the production environment. The Entity's CIP compliance program lacked strong internal controls related to configuration management. The lack of sufficient internal controls around configuration management and change management resulted in less than adequate procedures, insufficient oversight, and a lack of written documentation and communication about how to maintain security in accordance with the NERC Reliability Standards.

CIP-007-6 R5

WECC determined that The Entity failed to submit Technical Feasibility Exception (TFE) requests for Cyber Assets that were not capable of either limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts. The Cyber Assets in scope included [REDACTED] BES Cyber Assets (BCAs), [REDACTED] Protected Cyber Assets (PCAs), and [REDACTED] Physical Access Control Systems (PACS) associated with its [REDACTED] High Impact BES Cyber Systems (HIBCS) located at its primary and backup Control Centers.

The root cause of this violation was that The Entity lacked a documented process to perform routine oversight of the TFEs that had been filed or needed to be filed with WECC.

WECC determined that this violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 1 includes the facts regarding the violation that WECC considered in its risk assessment.

The Entity submitted its mitigation activities to address the referenced violation. Attachment 1 includes a description of the mitigation activities The Entity took to address this violation.

The Entity certified that it had completed all mitigation activities. WECC certified that The Entity had completed all mitigation activities on October 2, 2018. Attachment 1 provides specific information on WECC's verification of The Entity's completion of the activities.

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 4

CIP-010-2 R1

WECC determined that The Entity was in noncompliance with CIP-010-2 R1 in two separate violations.

WECC2018019192

WECC determined that The Entity failed to: (1) develop a baseline configuration that included applied security patches on Electronic Access Points (EAPs) and Electronic Access Control and Monitoring Systems (EACMS); (2) update the baseline configuration within 30 calendar days of completing a change that deviated from the existing baseline configuration on PCAs; and (3) test changes in a test or production environment that models the baseline configuration to ensure that the required cyber security controls for CIP-005-5 R1 Part 1.5 were not adversely affected. Additionally, The Entity failed to document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment.

The root cause of this violation was The Entity lacked, or had less than adequate, change control process documentation. Specifically, while The Entity had change control process documentation in place, it did not include all situations and requirements of CIP-010-2 R1 that described how to complete certain tasks based on specific situations or scenarios. In some cases, the documentation was not in place to help The Entity ensure tasks were implemented correctly. The Entity had multiple change control forms in place, which caused confusion and contributed to instances of tasks in specific situations or scenarios not being implemented correctly.

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 activities to address the referenced violation. Attachment 3b includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 3b.

The Entity certified that it had completed all mitigation activities. WECC verified that The Entity had completed all mitigation activities on January 8, 2019. Attachments 1 and 3d provide specific information on WECC's verification of The Entity's completion of the activities.

WECC2017018484

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 5

WECC determined that The Entity failed to develop baseline configurations for [REDACTED] HIBCS BCAs and [REDACTED] EACMS in the Demilitarized Zone (DMZ) associated with the HIBCS, which included the operating system or firmware where no independent operation system existed, as required by CIP-010-2 R1 Part 1.1 sub-part 1.1.1.

The root cause of this violation was that The Entity did not have proper procedures for personnel to follow. This resulted in an employee making the wrong decision regarding documenting baselines for the affected Cyber Assets.

WECC determined that this violation posed a moderate risk and did not pose 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 activities to address the referenced violation. Attachment 3f includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 3f.

The Entity certified that it had completed all mitigation activities. WECC verified that The Entity had completed all mitigation activities on August 6, 2019. Attachments 1 and 3h provide specific information on WECC's verification of The Entity's completion of the activities.

#### CIP-010-2 R2

WECC determined that The Entity was in noncompliance with CIP-010-2 R2 in two separate violations.

WECC2017018485

WECC determined that for two separate instances, The Entity failed to monitor, at least once every 35 calendar days, for changes to the baseline configurations, and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1. In one instance, The Entity missed one Polycom system classified as a PCA associated with the HIBCS during manual monitoring, 22 days past the requirement of at least once every 35 calendar days. In the second instance, The Entity discovered [REDACTED] virtual hosts ([REDACTED] BCAs and [REDACTED] EACMS) associated with the HIBCS that had not been monitored for baseline configuration changes 301 days past the requirement of at least once every 35 calendar days.

The root cause of the first instance of this violation was a software failure. Specifically, the SharePoint email reminder system stalled during an upgrade, which caused task notifications to fail.



NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 6

The root cause of the second instance of this violation was The Entity lacked written communication. Specifically, personnel did not have proper procedures to follow, which resulted in incorrect decisions regarding documenting baselines for these Cyber Assets, and thus baseline configuration changes were not monitored.

WECC determined this violation posed a moderate risk and did not pose 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 activities to address the referenced violation. Attachment 4b includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 4b.

The Entity certified that it had completed all mitigation activities. WECC verified that The Entity had completed all mitigation activities on September 20, 2018. Attachments 1 and 4d provide specific information on WECC's verification of The Entity's completion of the activities.

WECC2018019012

WECC determined that The Entity had not been monitoring [REDACTED] "active" BCAs for changes to logically accessible ports and services, due to an omission of the Cyber Assets from the manually populated vulnerability scanner asset list.

The root cause of the violation was that The Entity lacked written documentation or communication for responsible personnel to know that the BCAs required nightly scans. Specifically, prior to the violation, nightly scans were occurring on the BCAs. However, the analyst responsible for completing the monitoring was not aware that the BCAs required nightly scans and no documentation existed that stated they required nightly scans, so the analyst removed the scans from the vulnerability scanner asset list.

WECC determined that the violation posed a moderate risk and did not pose 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.

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 7

The Entity submitted its mitigation activities to address the referenced violation. Attachment 4f includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 4f.

The Entity certified that it had completed all mitigation activities. WECC certified that The Entity had completed all mitigation activities on December 19, 2018. Attachments 1 and 4h provide specific information on WECC's 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 three hundred seventy-eight thousand dollars (\$378,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered The Entity's compliance history with CIP-007-6 R5 as an aggravating factor in the penalty determination;<sup>5</sup>
2. WECC repeatedly requested information from The Entity and The Entity was indifferent both in the length of time it took and with information when responding to those requests, which impeded the review and resolution of violations WECC2017018484, WECC2017018485, WECC2018019012;
3. The Entity agreed to settle these violations and agreed to the monetary penalty;
4. The Entity accepted responsibility and admitted to the violations;
5. The Entity self-reported WECC2018019012 timely after discovery;
6. The Entity was cooperative during its WECC audit, which resulted in the timely resolution of WECC2018019376.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of three hundred seventy-eight thousand dollars (\$378,000) 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<sup>6</sup>**

##### **Basis for Determination**

---

<sup>5</sup> The Entity's relevant prior noncompliance with CIP-007-6 R5 include(s): NERC Violation ID [REDACTED]

<sup>6</sup> See 18 C.F.R. § 39.7(d)(4).

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 8

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,<sup>7</sup> the NERC BOTCC reviewed the violations on August 14, 2019 and approved the resolution between WECC and The Entity. In approving the resolution, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the resolution and believes that the assessed penalty of three hundred seventy-eight thousand dollars (\$378,000) 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 The Entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publicly, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the Notice of Penalty as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113, respectively.<sup>8</sup>

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

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

---

<sup>7</sup> *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).

<sup>8</sup> 18 C.F.R. § 388.113(e)(1).



## NERC Notice of Penalty

The Entity

October 31, 2019

Page 9

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

Consistent with its past practice, NERC is redacting information from this Notice of Penalty according to Section 39.7(b)(4) because it contains information that would jeopardize the security of the BPS if publicly disclosed. NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation.<sup>9</sup> Nonpublic treatment of redacted information, including the identity of The Entity and other details of the violations, depends on: 1) the nature of the CIP violations; 2) whether mitigation is complete; 3) the extent to which the disclosure of The Entity's identity would be useful to someone seeking to cause harm; 4) whether an audit has occurred since the violations; 5) whether the violations were administrative or technical in nature; and 6) the length of time that has elapsed since the filing of the Notice of Penalty.<sup>10</sup>

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

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.<sup>12</sup> 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.<sup>13</sup> Details about The Entity's systems, including specific configurations or the tools/programs

---

<sup>9</sup> In response to recent Freedom of Information Act requests, the Commission has directed public disclosure regarding the disposition of CIP violations. *See, e.g.*, Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-19 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). In those cases, the Commission directed public disclosure of the identity of the registered entity; the Commission did not disclose other details regarding the CIP violations.

<sup>10</sup> FOIA No. FY19-30, Second Notice of Intent to Release (June 13, 2019).

<sup>11</sup> *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104

<sup>12</sup> See the next section for a list of this information.

<sup>13</sup> See below for a list of this information.

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 10

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 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 specific cyber security issues and related vulnerabilities, as well as details concerning the types and configurations of The Entity's systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

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

1. BES Cyber System Information, including security procedures; information related to BES Cyber Assets; individual IP addresses with context; group of IP addresses; Electronic Security Perimeter diagrams that include BES Cyber Asset names, BES Cyber System names, IP addresses, IP address ranges; security information regarding BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, Electronic Access Control and Monitoring Systems that is not publicly available; and network topology diagrams, etc.
2. The names of The Entity's vendors and contractors.
3. The NERC Compliance Registry number of The Entity.
4. The registered function and registration date 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.

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 11

Under Section 388.113, NERC requests that the CEII designation apply to the redacted information in Item 1-2 for five years starting from this filing date, October 31, 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, October 31, 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 WECC.

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

#### **Attachments to be Included as Part of this Notice of Penalty**

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

1. Settlement Agreement by and between WECC and The Entity executed July 16, 2019, included as Attachment 1;
2. WECC's Audit Discovery Record of violation of CIP-007-6 R5 submitted March 14, 2018, included as Attachment 2;
3. The Entity's Self-Report of violation of CIP-010-2 R1 Part 1.5 submitted February 13, 2018, included as Attachment 3a;
4. The Entity's Mitigation Plan designated as WECCMIT014174-2 for CIP-010-2 R1 Part 1.5 submitted November 27, 2018, included as Attachment 3b;
5. The Entity's Certification of Mitigation Completion for CIP-010-2 R1 Part 1.5 submitted on November 27, 2018, included as Attachment 3c;
6. Verification of Mitigation Plan Completion for CIP-010-2 R1 Part 1.5 dated January 8, 2019, included as Attachment 3d;
7. The Entity's Self-Report of violation of CIP-010-2 R1 Part 1.1 submitted October 12, 2017, included as Attachment 3e;
8. The Entity's Mitigation Plan designated as WECCMIT014184 for CIP-010-2 R1 Part 1.1 submitted October 5, 2018, included as Attachment 3f;
9. The Entity's Certification of Mitigation Completion for CIP-010-2 R1 Part 1.1 dated November 7, 2018, included as Attachment 3g;

NERC Notice of Penalty

The Entity

October 31, 2019

Page 12

10. Verification of Mitigation Plan Completion for CIP-010-2 R1 Part 1.1 dated August 6, 2019, included as Attachment 3h;
11. The Entity's Self-Report of violation of CIP-010-2 R2 Part 2.1 submitted October 12, 2017, included as Attachment 4a;
12. The Entity's Mitigation Plan designated as WECCMIT013978-2 for CIP-010-2 R2 Part 2.1 submitted August 30, 2018, included as Attachment 4b;
13. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 Part 2.1 dated September 7, 2018, included as Attachment 4c;
14. Verification of Mitigation Plan Completion for CIP-010-2 R2 Part 2.1 dated September 20, 2018, included as Attachment 4d;
15. The Entity's Self-Report of violation of CIP-010-2 R2 submitted January 19, 2018, included as Attachment 4e;
16. The Entity's Mitigation Plan designated as WECCMIT014094 for CIP-010-2 R2 submitted August 31, 2018, included as Attachment 4f;
17. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R2 submitted November 27, 2018, included as Attachment 4g;
18. Verification of Mitigation Plan Completion for CIP-010-2 R2 dated December 19, 2018, included as Attachment 4h.

NERC Notice of Penalty  
 The Entity  
 October 31, 2019  
 Page 13

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

<p>*Persons to be included on the Commission’s service list are indicated with an asterisk. NERC requests waiver of the Commission’s rules and regulations to permit the inclusion of more than two people on the service list.</p>	<p>Edwin G. Kichline*          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</p>
<p>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</p>	<p>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</p>
<p>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</p>	
<p>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</p>	





NERC Notice of Penalty

The Entity

October 31, 2019

Page 14

NERC Notice of Penalty  
The Entity  
October 31, 2019  
Page 15

## 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:

  
WECC

Attachments

Attachment 1

Settlement Agreement by and between WECC  
and The Entity executed July 16, 2019



CONFIDENTIAL

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

June 27, 2019

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

Subject: Notice of Expedited Settlement Agreement

[REDACTED]

## I. Introduction

The Western Electricity Coordinating Council (WECC) hereby notifies [REDACTED] [REDACTED] ([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 Requirement	NERC Violation ID	WECC Violation ID
CIP-007-6 R5	WECC2018019376	WECC2018-614869
CIP-010-2 R1	WECC2018019192	WECC2018-614816
CIP-010-2 R1	WECC2017018484	WECC2017-614668
CIP-010-2 R2	WECC2017018485	WECC2017-614669
CIP-010-2 R2	WECC2018019012	WECC2018-614764

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 \$378,000.

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)<sup>1</sup>, 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 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.

---

<sup>1</sup> "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))





CF1492

June 27, 2019

WECC's determination of penalties 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 15 calendar days from the date of this Notice.

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

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

#### V. Disclosure Notice

NERC may include 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 business days after the date of this Notice.

#### 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.

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](mailto:dhorvath@wecc.org).



CF1492

June 27, 2019

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 and takes responsibility for the violations of the NERC Reliability Standards listed addressed herein.
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, 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.
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. To settle these matters, [REDACTED] hereby agrees to pay \$378,000 to WECC via wire transfer or cashier's check. [REDACTED] shall make the funds payable to a WECC account identified in a Notice of Payment Due that WECC will send to [REDACTED] upon approval of this Settlement Agreement by NERC and FERC. [REDACTED] shall issue the payment to WECC no later than thirty days after receipt of the Notice of Payment Due. If this payment is not timely received, WECC shall assess, and [REDACTED] agrees to pay, an interest charge calculated according to the method set forth at 18 CFR §35.19(a)(2)(iii) beginning on the 31<sup>st</sup> day following issuance of the Notice of Payment Due.
12. In addition, [REDACTED] must submit Mitigation Plans within 30 calendar days 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 STANDARD CIP-007-6 REQUIREMENT 5**

NERC VIOLATION ID: WECC2018019376

WECC VIOLATION ID: WECC2018-61489

**STANDARD**

14. NERC Reliability Standard CIP-007-6 Requirement 5 states:

*R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.*

*Part 5.7. Where technically feasible, either:*

- *Limit the number of unsuccessful authentication attempts; or*
- *Generate alerts after a threshold of unsuccessful authentication attempts.*

**STIPULATED VIOLATION FACTS**

15. During a Compliance Audit conducted [REDACTED], WECC determined the entity, as a [REDACTED], had a potential noncompliance of CIP-007-6 R5.

16. Specifically, WECC determined the entity failed to submit a Technical Feasibility Exception (TFE) request for Cyber Assets that were not capable of either limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts. The Cyber Assets in scope included [REDACTED] BES Cyber Assets (BCAs), [REDACTED] Protected Cyber Assets (PCAs), and [REDACTED] Physical Access Control Systems (PACS) associated with its [REDACTED] High Impact BES Cyber Systems (HIBCS) located at its primary and backup Control Centers. The entity confirmed during its audit and during subsequent conversations with WECC that these [REDACTED] Cyber Assets had no External Routable Connectivity (ERC) and were not capable of meeting the requirement of Part 5.7. Additionally, the entity believed at the time of the violation an existing WECC approved TFE submitted under Version 3 of the CIP Standards applied to the Cyber Assets in scope, when in fact there were no TFE's approved by WECC for CIP-007-6 R5 Part 5.7 that included the Cyber Assets in scope of this violation.

17. After reviewing all relevant information, WECC Enforcement concurs with the audit finding. The entity failed CIP-007-6 R5 Part 5.7 as described above.

18. The root cause of the violation was the lack of a documented process to perform routine oversight of the TFEs that had been filed or needed to be filed with WECC.





19. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 10, 2018, when the entity submitted a TFE request with WECC for the Cyber Assets, for a total of 679 days of noncompliance.

### RELIABILITY RISK ASSESSMENT

20. WECC determined the violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to submit a TFE request for Cyber Assets that were not capable of either limiting the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful authentication attempts as required by CIP-007-6 R5 Part 5.7.
21. However, as compensating controls, the entity had implemented password length and complexity that was beyond what was required for compliance with the NERC CIP Standards; the entity's account management system generated random passwords; the Cyber Assets in scope of this violation did not have ERC, therefore anyone with malicious intent would have to gain physical access to the Cyber Assets in order to attempt to login; and the entity's physical access controls were confirmed to be compliant during the audit. No harm is known to have occurred.

### REMEDIATION AND MITIGATION

22. On August 8, 2018, the entity completed mitigating activities to address its violation and on October 2, 2018, WECC verified completion of the entity's mitigating activities.
23. To remediate and mitigate this violation, the entity:
- submitted TFE requests for the Cyber Assets in scope of this violation;
  - updated its TFE procedure; and
  - sent an email to personnel to notify them of the new procedure with instructions to review the procedure.

### **B. NERC RELIABILITY STANDARD CIP-010-2 REQUIREMENT 1**

NERC VIOLATION ID: WECC2018019192

WECC VIOLATION ID: WECC2018-614816

### STANDARD

24. NERC Reliability Standard CIP-010-2 Requirement 1 states:
- 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.*

*Part 1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.*

*Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration:*

*1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and*

*1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.*

## **STIPULATED VIOLATION FACTS**

25. On February 13, 2018, the entity submitted a Self-Report stating, as an [REDACTED] it was in violation of CIP-010-2 R1.
  
26. Specifically, on December 15, 2017, during a routine reconciliation of baseline deviations the entity discovered three baseline configurations had not been updated within 30 calendar days of completing a change, in violation of CIP-010-2 R1 Part 1.3. One of the previous changes occurred on October 10, 2017 and the other two changes occurred on December 14, 2017. The scope of this issue included [REDACTED] PCAs associated with the HIBCS. Failing to update the baseline configuration within 30 days could possibly have caused the entity to not be aware of significant changes to the baseline of the Cyber Assets, which could have resulted in changes being approved without knowledge of the existing configuration. A change could potentially be approved and added



without complete knowledge of the current network ports, firmware, operating systems, and configuration details. This could cause the entity to be unaware of the current authorized and enabled configuration, firmware, or operating system details.

27. Additionally, on February 9, 2018, [REDACTED] the entity identified several instances of noncompliance. First, the entity identified it had not developed baseline configurations for applied security patches for [REDACTED] network-based appliances, in violation of CIP-010-2 R1 Part 1.1 sub-part 1.1.5. The scope of this issue included [REDACTED] Electronic Access Points (EAPs) and [REDACTED] Electronic Access Control and Monitoring Systems (EACMS) associated with the HIBCS. By failing to document the applied security patches in the baseline configuration, the entity may be unaware of the current security patches installed. This could have caused misinformation and confusion when the entity looked at the current security patches on the Cyber Assets, resulting in applicable security patches not being applied to EACMS. This could leave vulnerabilities on the EACMS as well as the EAP to the ESP of the entity's HIBCS, which could result in potentially having an [REDACTED]

28. Second, the entity identified [REDACTED] times where testing of changes did not include validation and documentation of required cyber security controls testing prior to adding the change into production, in violation of CIP-010-2 R1 Part 1.5 sub-parts 1.5.1 and 1.5.2. The scope of this issue included [REDACTED] BCAs in the HIBCS. Failing to test changes to BCAs prior to implementing the change in production, to ensure that CIP-005 security controls are not adversely affected could potentially cause these security controls to not be verified resulting in significant adverse effects; malicious code may be introduced into the HIBCS production environment; incompatibility of new and existing configurations resulting in Cyber Asset outages or inoperability; both examples potentially resulting in affecting the BES and other entities within the western Interconnection.

29. [REDACTED]

30. After reviewing all relevant information, WECC determined the entity failed:
- a. to develop a baseline configuration which included applied security patches on [REDACTED] EAPs and [REDACTED] EACMS, as required by CIP-010-2 R1 Part 1.1 sub-part 1.1.5;
  - b. to update the baseline configuration within 30 calendar days of completing a change that deviated from the existing baseline configuration on [REDACTED] PCAs, as required by CIP-010-1 R1 Part 1.3;



- c. to test changes in a test or production environment that models the baseline configuration to ensure that the required cyber security controls for CIP-005-5 R1 Part 1.5 were not adversely affected, document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, for [REDACTED] changes associated with [REDACTED] BCAs, as required by CIP-010-2 R1 Part 1.5 sub-parts 1.5.1 and 1.5.2, respectively.
31. The root cause of the violation was a lack of, or less than adequate, change control process documentation. Specifically, where the entity had change control process documentation in place, it did not include all situations and requirements of CIP-010-2 R1 that described how to complete certain tasks based on specific situations or scenarios. In some cases, the documentation was not in place to help the entity ensure tasks were implemented correctly. The entity had multiple change control forms in place which caused confusion and contributed to these instances.
  32. This violation started on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on November 20, 2018, when the entity addressed and completed remediation, for a total of 873 days of noncompliance.

### RELIABILITY RISK ASSESSMENT

33. WECC determined this violation posed a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed:
  - a. to update the baseline configuration within 30 calendar days of completing a change that deviated from the existing baseline configuration on [REDACTED] PCAs, as required by CIP-010-1 R1 Part 1.1 Sub- Part 1.1.5;
  - b. to develop a baseline configuration which included applied security patches on [REDACTED] EAPs and [REDACTED] EACMS, as required by CIP-010-2 R1 Part 1.3; and
  - c. to test changes in a test or production environment that models the baseline configuration to ensure that the required cyber security controls for CIP-005-5 R1 Part 1.5 were not adversely affected, and document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments for [REDACTED] changes associated with [REDACTED] BCAs, as required by CIP-010-2 R1 Part 1.5 sub-parts 1.5.1 and 1.5.2, respectively.
34. The entity had not implemented any detective controls and had weak preventive controls. However, as compensation, the entity utilized a scanning tool which ran daily to ensure that



system baselines were consistent. The entity also monitored all access permissions to identify discrepancies between authorized and unauthorized permissions. Scripts for permissions were run twice daily. Nevertheless, no harm is known to have occurred.

### REMEDIATION AND MITIGATION

35. On November 27, 2018, the entity submitted a Mitigation Plan to address its violation and on December 5, 2018, WECC accepted the entity's Mitigation Plan.

36. To remediate and mitigate this violation, the entity:

- a. validated that the test environment was not different than the production environment, related to the BCAs;
- b. updated baseline configurations for all applicable PCAs;
- c. created baseline configurations for the network based appliances on the EACMS;
- d. developed a Baseline Management Plan (Plan) and associated documents;
- e. provided training to change control implementers on the Plan and associated documents, and obtained signatures acknowledging review of the Plan and associated documents;
- f. merged the change control form into one form which places a control in-between the testing and implementation-to-production phase. It also streamlines the process for the change control implementer and makes oversight of the ticket more efficient;
- g. created two reports; one to track baselines that need updating after the work has been completed, and one to track the Compliance Security analyst review of the updated baselines. These two reports are emailed to appropriate personnel daily; and
- h. updated the compliance dashboard in SharePoint with the two new CIP-010-2.

37. On November 27, 2018, the entity submitted a Mitigation Plan Completion Certification and on January 8, 2019 WECC verified the completion of its Mitigation Plan.

### **C. NERC RELIABILITY STANDARD CIP-010-2 REQUIREMENT 1**

NERC VIOLATION ID: WECC2017018484

WECC VIOLATION ID: WECC2017-614668

### **STANDARD**

38. NERC Reliability Standard CIP-010-2 Requirement 1 states:

*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.*

### **STIPULATED VIOLATION FACTS**

39. On October 12, 2017, the entity submitted a Self-Report stating, as an [REDACTED] it was in violation of CIP-010-2 R1.
40. Specifically, on May 29, 2017, during the development of the programmatic node validation, it was discovered that baseline configurations for [REDACTED] HIBCS BCAs and [REDACTED] EACMS in the Demilitarized Zone (DMZ) associated with the HIBCS, had not been developed. The lack of documented baselines and monitoring could result in the devices running vulnerable software/firmware that could lead to compromise of these systems. This potential compromise could result in a malicious actor gaining full control of the Cyber Assets and exposing all hosts that are deployed on these systems including [REDACTED] total virtual hosts.
41. After reviewing all relevant information, WECC determined the entity failed to develop a baseline configuration, individually or by group, which included the operating system (including version) or firmware where no independent operating system exists, as required by CIP-010-2 R1 Part 1.1 sub-part 1.1.1.
42. The root cause of the violation was entity personnel did not have proper procedures to follow, which resulted in an incorrect decision regarding documenting baselines for these Cyber Assets.
43. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on June 1, 2017, when the entity developed baseline configurations for the Cyber Assets in scope, which included the operating system, for a total of 336 days of noncompliance.

### **RELIABILITY RISK ASSESSMENT**





44. WECC determined this violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to develop a baseline configuration, individually or by group, which included the operating system (including version) or firmware where no independent operating system exists, as required by CIP-010-2 R1 Part 1.1 sub-part 1.1.1.
45. The entity had not implement effective detective controls. Specifically, this instance was discovered over a year after the start date. However, as compensation, the entity utilized a scanning tool which ran daily to ensure that system baselines were consistent. The entity also monitored all access permissions to identify discrepancies between authorized and unauthorized permissions. Scripts for permissions were run twice daily. Nevertheless, no harm is known to have occurred.

### **REMEDATION AND MITIGATION**

46. On October 5, 2018, the entity submitted a Mitigation Plan to address its violation and on November 15, 2018, WECC accepted the entity's Mitigation Plan.
47. To remediate and mitigate this violation, the entity:
- a. developed baseline configurations for the Cyber Assets in scope, to include the operating systems;
  - b. automated the Cyber Asset verification of inventory which will help determine which Cyber Assets do not have a baseline configuration. An e-mail notification is sent to appropriate personnel if an asset requires a baseline and/or needs an update;
  - c. updated its Change Control Procedure to include a section on deploying new assets, which shows that for new assets, if the baseline does not match the existing baseline of a similar asset, a new baseline must be created. There is also a process for a new asset in that the baseline configuration must be finalized prior to the deployment into production;
  - d. updated its Baseline Management Plan; Baseline Update Procedure, and Change Control and Configuration Management Policy to include roles and responsibilities; and
  - e. provided training to applicable personnel on all updated documentation.
48. On November 7, 2018, the entity submitted a Mitigation Plan Completion Certification and on December 12, 2018, WECC verified the completion of its Mitigation Plan.

#### **D. NERC RELIABILITY STANDARD CIP-010-2 REQUIREMENT 2**

NERC VIOLATION ID: WECC2017018485

WECC VIOLATION ID: WECC2017-614669



### STANDARD

49. NERC Reliability Standard CIP-010-2 Requirement 2 states:

*R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-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

50. On October 12, 2017, the entity submitted a Self-Report stating, as an [REDACTED] it was in violation of CIP-010-2 R2.

51. Specifically, on August 15, 2017 the entity began manual monitoring for changes to baseline configurations when it discovered that the SharePoint workflow email reminder had stalled during a SharePoint version upgrade. One Polycom system classified as a PCA associated with the HIBCS was missed during the manual monitoring. The manual monitoring for the PCA was completed on August 15, 2017, 22 days past the requirement of at least once every 35 calendar days. The entity did not detect any unauthorized changes to the PCA baseline configuration. Additionally, on September 28, 2017, the entity discovered [REDACTED] virtual hosts ([REDACTED] BCA's and [REDACTED] EACMS) associated with the HIBCS that had not been monitored for baseline configuration changes since August 5, 2016. The entity began manual monitoring of these Cyber Assets on July 10, 2017, 301 days past the requirement of at least once every 35 calendar days. The entity did not detect any unauthorized changes to these Cyber Asset baseline configurations. The failure to monitor baselines created risk to the individual Cyber Assets as well as the respective systems in which these devices were deployed. This issue could have caused the entity to be unaware of any authorized and unauthorized changes, resulting in the Cyber Assets running vulnerable software/firmware that could compromise the systems, such as loss of control of the Cyber Assets and exposing all hosts that are deployed on these systems, including [REDACTED] total virtual hosts; [REDACTED] Cisco BCA and [REDACTED] EACMS. Additionally, the potential result of compromise could have been the complete control (installation of software, exfiltration of data, remote control, etc.) of the affected system and an anchor point for reconnaissance and spreading of malware through the environment, which could have severe negative effects on the entity's connected BCS.

52. After reviewing all relevant information, WECC determined that for two separate instances the entity failed to monitor at least once every 35 calendar days for changes to the baseline



configurations, and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.

53. The root cause of the first instance was a software failure. Specifically, the SharePoint email reminder system stalled during an upgrade which caused task notifications to fail.
54. The root cause of the second instance was a lack of written communication. Specifically, personnel did not have proper procedures to follow which resulted in them making incorrect decisions regarding documenting baselines for these Cyber Assets, that lead to not monitoring baseline configuration changes.
55. The first instance began on July 25, 2017, the day after the last day when monitoring to baseline changes should have occurred for the PCA, and ended on August 15, 2017, when the entity began monitoring baseline configuration changes on the PCA, for a total of 22 days of noncompliance.
56. The second instance began on August 5, 2016, when the initial performance of the Standard and Requirement should have been completed for the virtual hosts should have occurred, and ended on June 1, 2017, when the entity began monitoring baseline configuration changes on the virtual hosts, for a total of 301 days of noncompliance.

#### **RELIABILITY RISK ASSESSMENT**

57. WECC determined these instant violations posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. For the two instances, the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.
58. However, the entity implemented strong controls. Its network was monitored 24 hours a day, seven days a week, year-round via manned personnel. Automated scripts ran twice daily to validate authorized accounts and permission on all Cyber Assets. Additionally, the rights to the servers were granted utilizing an employee management tool to ensure that only authorized users were able to access systems. Changes were not made to systems unless a change management ticket was input and approved. The virtual host servers resided within a controlled, secured network, and were monitored and logged. The baseline scans did not include the virtual host servers in scope of this violation. The entity implemented strong compensating controls in that although the baseline configurations had not been developed for the virtual host servers, they had security patch checks performed automatically and no changes were identified during the noncompliance. No harm is known to have occurred.



## **REMEDATION AND MITIGATION**

59. On August 30, 2018, the entity submitted a Mitigation Plan to address its violation and on September 4, 2018, WECC accepted the entity's Mitigation Plan.

60. To remediate and mitigate this violation, the entity:

- a. performed baseline configuration change reviews on all Cyber Assets in scope in order to document and investigate detected unauthorized changes. No changes detected;
- b. began monitoring for changes to the baseline configurations on the Cyber Assets;
- c. automated its node validation report by creating a report that automates the cross check of node membership, the Cyber Asset List, and the manual baseline review list. This report shows the status of node membership and if there are any failures that need to be addressed. This report will show if there are any devices that do not have a baseline or if a device is not found in the node membership;
- d. developed and implemented a compliance dashboard email report to monitor the status of manual baseline review due dates, mitigation plan due dates, and security patch review due dates. The compliance dashboard shows baselines that are required to be reviewed, and the amount of days left to review and monitor the baselines. Once the days past column gets closer to the day the baseline is due to be reviewed, it changes colors from green, to yellow, to red. It is also emailed twice a week notifying them when baselines are due to be reviewed; and
- e. completed training that included CIP-010-2 R2 change control and configuration management monitoring reviews, roles and responsibilities, workflow e-mail reminders, and the compliance reports. The compliance reports include a dashboard of the number of days until the baseline review needs to be completed and who is responsible for performing the review.

61. On September 7, 2018, the entity submitted a Mitigation Plan Completion Certification and on September 13, 2018, WECC verified the completion of its Mitigation Plan.

### **E. NERC RELIABILITY STANDARD CIP-010-2 REQUIREMENT 2**

NERC VIOLATION ID: WECC2018019012

WECC VIOLATION ID: WECC2018-614764

## **STANDARD**

62. NERC Reliability Standard CIP-010-2 Requirement 2 states:



R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-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**

63. On January 19, 2018, the entity submitted a Self-Report stating, as an [REDACTED] it was in violation of CIP-010-2 R2.
64. Specifically, on January 15, 2018, during a review of its Cyber Asset list the entity discovered a media workstation console, classified as a BCA associated with the HIBCS, was set up to be monitored by the vulnerability scanner, but had been inadvertently set to "inactive" on September 29, 2017. The console sends call control instructions on behalf of the media workstation. Initial review revealed that the BCA had not been monitored for changes to logically accessible ports and services since February 6, 2017. An immediate review of all assets monitored in the vulnerability scanner was then performed. The review revealed an additional [REDACTED] "active" BCAs that had not been monitored since February 6, 2017. The BCA baseline configurations were not monitored due to an omission of the Cyber Assets from the manually populated vulnerability scanner asset list. A failure to monitor a baseline for unauthorized changes could have allowed someone with malicious intent to change configuration or enable a port on the Cyber Asset without the entity being aware of the changes, which could result in the devices not functioning as intended or becoming inoperable. This could have also resulted in a negative impact on the HIBCS and entity communications which are critical for the reliability function for which the entity is responsible.
65. After reviewing all relevant information, WECC determined the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.
66. The root cause of the violation was the lack of written documentation or communication. Specifically, prior to the violation, nightly scans were occurring on the BCAs. However, the analyst responsible for completing the monitoring was not aware that the BCAs required nightly scans and no documentation existed that stated they required nightly scans, so the analyst removed them from the vulnerability scanner asset list.
67. This violation began on March 14, 2017, the day after the last day monitoring for baseline configuration changes should have occurred for the BCAs, and ended on January 16, 2018, when



the entity began monitored baseline configuration changes on the affected BCAs, for a total of 309 days of noncompliance.

### RELIABILITY RISK ASSESSMENT

68. WECC determined this violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, and document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.
69. However, the entity implemented good compensating controls. Specifically, it ensured that only authorized users were able to access systems. Changes were not made to systems unless a change management ticket had been input and approved. Additionally, the BCAs in scope were on a separate network than the EMS. Nevertheless, no harm is known to have occurred.

### REMEDIATION AND MITIGATION

70. On August 31, 2018, the entity submitted a Mitigation Plan to address its violation and on November 13, 2018, WECC accepted the entity's Mitigation Plan.
71. To remediate and mitigate this violation, the entity:
- a. reviewed the BCAs in scope for logically accessible ports and services. No unauthorized changes to the baseline configurations were discovered during this review;
  - b. verified scope to ensure that all Cyber Assets with baselines monitored for unauthorized changes to the logically accessible ports and services were scanned by the vulnerability scanner. No additional Cyber Assets identified;
  - c. developed and implemented a weekly automated reconciliation of Cyber Assets scanned by the vulnerability scanner to verify that all Cyber Assets requiring monitoring of logical ports and services were successfully scanned using the vulnerability scanner logs. An email is sent to appropriate personnel if a Cyber Asset has not been scanned within the last 48 hours from the CIP-010-2 baseline monitoring system; and
  - d. created a Cyber Asset inventory site population script to programmatically generate a list of IP addresses for Cyber Assets scanned by the vulnerability scanner from the Cyber Asset List created and provided to the Compliance Security Analyst responsible for managing the port monitoring scans performed using the vulnerability scanner.
72. On November 27, 2018, the entity submitted a Mitigation Plan Completion Certification and on December 12, 2018, WECC verified the completion of its Mitigation Plan.





**PROPOSED PENALTY OR SANCTION**

73. WECC determined that the proposed penalty of \$378,000 is appropriate for the following reasons:

- a. Base penalty factors:
  - i. The Violation Risk Factor (VRF), Violation Severity Level (VSL), and risk to the reliability of the BPS are as described in Table 1.

Table 1

<b>Standard Requirement</b>	<b>NERC Violation ID</b>	<b>VRF</b>	<b>VSL</b>	<b>Risk to the Reliability of the BPS</b>
CIP-007-6 R5	WECC2018019376	Medium	Severe	Minimal
CIP-010-2 R1	WECC2018019192	Medium	Severe	Serious
CIP-010-2 R1	WECC2017018484	Medium	Severe	Moderate
CIP-010-2 R2	WECC2017018485	Medium	Severe	Moderate
CIP-010-2 R2	WECC2018019012	Medium	Severe	Moderate

- ii. All the violations have an Operations Planning violation time horizon expectation for remediation within the timeframe of the next day, up to and including the quarter, to preserve the reliability of the BPS.

Table 2

<b>Standard Requirement</b>	<b>NERC Violation ID</b>	<b>Start Date</b>	<b>End Date</b>	<b>Duration in Days</b>
CIP-007-6 R5	WECC2018019376	7/1/2016	5/10/2018	679
CIP-010-2 R1	WECC2018019192	7/1/2016	11/20/2018	873
CIP-010-2 R1	WECC2017018484	7/1/2016	6/1/2017	336
CIP-010-2 R2	WECC2017018485	#1 - 7/25/2017	8/15/2017	22
		#2 - 8/5/2016	6/1/2017	301
CIP-010-2 R2	WECC2018019012	3/14/2017	1/16/2018	309

- b. WECC applied a mitigating credit for the following reasons:
  - i. The entity agreed to settle these violations and penalty.
  - ii. The entity accepted responsibility and admitted to the violations.
  - iii. The entity Self-Reported WECC2018019012 timely after discovery.
  - iv. The entity was cooperative during its WECC audit which resulted in NERC Violation WECC2018019376.
- c. WECC applied an aggravating factor for the following reasons:
  - i. WECC considered the entity’s compliance history for CIP-007-6 R5, given violation IDs [REDACTED] and [REDACTED], to be relevant and applicable to the violations of this Settlement Agreement.



- ii. WECC repeatedly requested information from the entity and the entity was indifferent both in the length of time it took and with information when responding to those requests, which impeded the review and resolution of the violations listed in Table 3 below.

d. Other Considerations:

- i. WECC escalated the disposition treatment for the three Moderate risk violations, because the entity did not address the violations, determine the facts, or correct the problems in a timely manner. This was evident by the duration between the Self-Report submittal date and the Mitigation Plan submittal date as described in Table 3, and the violation duration as described in Table 2 above.

Table 3

Standard Requirement	NERC Violation ID	Self-Report Submittal Date	MP Submittal Date	Duration in Days
CIP-010-2 R1	WECC2017018484	10/12/2017	10/5/2018	359
CIP-010-2 R2	WECC2017018485	10/12/2017	8/30/2018	323
CIP-010-2 R2	WECC2018019012	1/19/2018	8/31/2018	225

- ii. WECC considered the entity’s compliance history for CIP-007-6 R5 and determined that the prior noncompliance was distinct, separate, and not relevant to the CIP-007-6 R5 violation in this Notice for the following reasons:
  - a. Violation ID [REDACTED] was related to a failure to provide adequate training
  - b. Violation ID [REDACTED]: was related to a failure to have an approved documented policy to manage administrator, shared, and other generic account privileges.
- i. WECC considered the entity’s compliance history for CIP-010-2 R1 given violation ID [REDACTED] and determined that the prior noncompliance, which was related to a documentation issue, was distinct, separate, and not relevant to the violation in this Settlement Agreement.
- ii. WECC did not apply a mitigating credit for cooperation for three of the violation in this Notice because the entity did not quickly address the violations, determine the facts, report, and correct the problems. This was evident by the duration between the Self-Report submittal date and the Mitigation Plan submittal date as described in Table 3 above.



- iii. WECC did not apply mitigating credit for the entity's Internal Compliance Program. Although the entity has a documented ICP, WECC determined the entity did not implement its ICP with effective internal controls sufficient to prevent and detect four of the five violations, thereby reducing the risk to the BPS. This was evident by the violation duration as described in Table 3 above.
- iv. Upon undertaking the actions outlined in the Mitigation Plan, the entity took voluntary corrective action to remediate these violations and did not have to be compelled to do so.

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

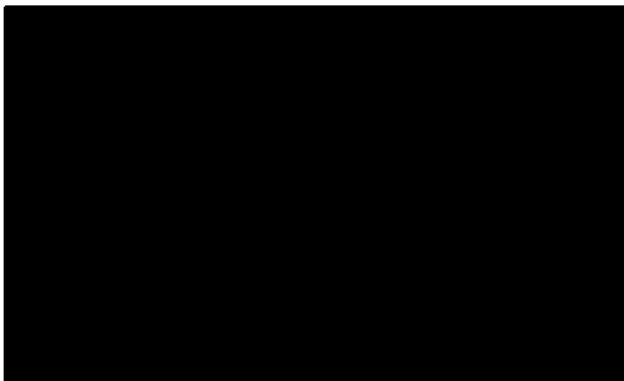


Agreed to and Accepted by:

WESTERN ELECTRICITY COORDINATING COUNCIL

  
\_\_\_\_\_  
Heather M. Laws  
Director, Enforcement

7-16-19  
\_\_\_\_\_  
Date



\_\_\_\_\_  
Date 07/15/2019

Attachment 2

WECC's Audit Discovery Record of violation of  
CIP-007-6 R5 submitted March 14, 2018

Violation - Discovery Record

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

NERC Violation ID:

Discovery Method: Audit

Date Submitted: March 14, 2018

Region Contact: Mailee Cook

Phone: 801-883-6866 Email: mcook@wecc.biz

Standard: CIP-007-6 - Cyber Security — System Security Management

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Requirement: CIP-007-6 R5.

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.

Violated Sub- Requirement(s): CIP-007-6 5.7.

Violated Function(s): [REDACTED]

Init Determ a Vltr: March 02, 2018

Begin Date of Vltr: July 01, 2016

End Date:

Notified of Vltr on: March 02, 2018

Potential Impact to Preventative:

BES: The entity implemented Good preventative control(s). Specifically, the entity implemented strict access controls restricting access into its ESPs. Additionally, the entity enforces password lengths and password changes beyond what is required by the Standard.

Compensating:

The entity implemented Good compensating control(s). Specifically, the entity implemented strict access controls restricting access into its ESPs. Additionally, the entity enforces password lengths and password changes beyond what is required by the Standard. All passwords on devices are randomly generated by its account management system

Corrective:

The entity implemented Good corrective control(s). Specifically, the entity the entity enforces password lengths and password changes beyond what is required by the Standard. The entity uses several tools to automate password changes. All passwords on devices are randomly generated by its account management system

Detective:

The entity implemented Weak detective control(s). The auditors did not note any detective controls on these devices.



Brief Vltm Descr. & The entity failed to submit Technical Feasibility Exceptions for [REDACTED] Cyber Assets which were incapable  
Cause: of limiting or generating alerts after a threshold of unsuccessful authentication attempts.

Alleged Violation:

Registered Entity  
Report/Response:

Risk Factor: Medium

Severity Level: VSL - Lower

Factual Basis: Source: <http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx>

PNC Risk Factor: Medium, 2/15/2018

PNC Severity Level: Lower (None of the examples provided in the VSL matched the potential noncompliance), 2/5/2018

Attachment 3

3a. The Entity's Self-Report of violation of CIP-010-2 R1

Part 1.5 submitted February 13, 2018

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-010-2

Requirement: CIP-010-2 R1.

Date Submitted: February 13, 2018

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date: April 17, 2017

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: [REDACTED]

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

Which Regions:

Date Reported to Regions:

Detailed Description and [REDACTED]

Cause of Possible Violation: As defined in NERC Reliability Standard CIP-010-2, Requirement 1.5, Where technically feasible, for each change that deviates from the existing baseline configuration: Part 1.5.1, Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects; that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and Part 1.5.2, Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.  
When preparing a WECC audit data request response, [REDACTED] instances were identified that indicated testing of changes did not include validation and documentation of required cyber security controls testing.  
[REDACTED] subsequently convened its Compliance Committee to review the issue and determined a potential violation of NERC Reliability Standard CIP-010-2 Requirement 1, Parts 1.5.1 and 1.5.2 exists. In demonstration of [REDACTED] Culture of Compliance, [REDACTED] is self-reporting the potential violations of Parts 1.5.1 and 1.5.2.

Self Report

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Mitigation: 1. Develop and implement a Baseline Management Plan by May 1, 2018 which includes all baseline management processes including testing and documentation.

- a. Process will include verification that each production change management ticket that affects CIP-010 baselines has an associated test ticket and that the testing is documented or that a plan to test changes in the production environment so that the test is performed in a manner that minimizes adverse effects
- b. Provide training on processes and procedures for all personnel with baseline management task roles and responsibilities by May 1, 2018.
- c. Combine test and production tickets into one change management ticket to allow the use of internal controls between the test and production implementation phases by May 1, 2018

Have Mitigating Activities been Completed? No

Date Mitigating Activities Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Moderate

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Testing did not include validation and documentation of required cyber security controls. However, no adverse effects occurred

Risk Assessment of Impact to BPS: Testing did not include validation and documentation of required cyber security controls

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  
WECCMIT014174-2 for CIP-010-2 R1 Part 1.5  
submitted November 27, 2018

## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: WECCMIT014174-2

Mitigation Plan Version: 3

NERC Violation ID	Requirement	Violation Validated On
WECC2018019192	CIP-010-2 R1.	09/04/2018

Mitigation Plan Submitted On: November 27, 2018

Mitigation Plan Accepted On: December 05, 2018

Mitigation Plan Proposed Completion Date: November 20, 2018

Actual Completion Date of Mitigation Plan: November 20, 2018

Mitigation Plan Certified Complete by [REDACTED] On: November 27, 2018

Mitigation Plan Completion Verified by WECC On: January 08, 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: Manager of Compliance

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		
WECC2018019192	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:

While preparing a WECC audit data request response, [REDACTED] discovered the following:

- [REDACTED] instances that indicated testing of changes did not include validation and documentation of required cyber security control testing. In each instance, the CIP-005 and CIP-007 security controls were validated during the production implementation of the ticket. In all but one instance, the control which was not validated during the testing process was CIP-007-6 R2.1 - R2.4. These requirements are administrative controls for the management of vulnerabilities. As individual system configurations are not part of this requirement, the control for the test systems was validated when patch tracking entries were provided as part of the CIP-007 R2.1-R2.4 security control validation for the production implementation. The remaining instance did not validate CIP-005-5 R1.5 security control. However, CIP-005-5 R1.5 was validated and evidence retained for the implementation of this change on cyber assets under the scope of NERC CIP.
- [REDACTED] instances where the applied security patch baseline configuration for [REDACTED] and [REDACTED] ([REDACTED]) had not been developed.

Additionally on December 15, 2017 when the Compliance Security Analyst was performing routine compliance oversight by reconciling baseline deviations reported by [REDACTED] it was discovered that two baseline configurations (three software updates) hadn't been updated within 30 calendar days. The dates of the last updates for the baselines were October 10th, 2017 and October 17, 2017.

Investigation lead to the conclusion that the root cause identified was a lack of expectations and a formalized process in all cases above.

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

See above

## 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. Discovery: Testing of changes did not include validation and documentation.

While preparing a [REDACTED], [REDACTED] identified [REDACTED] instances that the testing of changes did not include validation and documentation of required cyber security control testing.

Mitigation: In each instance, the CIP-005 and CIP-007 security controls were validated during the production implementation of the ticket. In all but one instance, the control which was not validated during the testing process was CIP-007-6 R2.1 - R2.4. These requirements are administrative controls for the management of vulnerabilities. The one remaining instance control for the test system was validated when patch tracking entries were provided as part of the CIP-007 R2.1-R2.4 security control validation for the production implementation.

Please see folder: [REDACTED]

2. Discovery: Security patch baseline configurations not developed

While preparing a [REDACTED], [REDACTED] identified two instances where the applied security patch baseline configuration for [REDACTED] and [REDACTED] had not been developed. These two instances were spread across [REDACTED] EACMs and [REDACTED] EAP categorized cyber assets.

Mitigation: Develop baseline and configure for monitoring

On March 15, 2018, the [REDACTED] baseline configuration was created and [REDACTED] was configured to monitor applied security patches

Please see: [REDACTED] and [REDACTED]

On March 26, 2018, the [REDACTED] baseline configuration was created and on March 27, 2018 [REDACTED] was configured to monitor applied security patches.

Please see: [REDACTED]

3. Discovery: Baseline configurations not updated within 30 calendar days

On December 15, 2017 the Compliance Security Analyst was performing routine oversight and discovered two baseline configurations (three software updates, one baseline had two software updates) hadn't been updated within 30 calendar days for [REDACTED] PCAs.

Mitigation: Baseline configurations updated

On December 15, 2017, the Compliance Security Analyst updated the baseline configurations

Please see: [REDACTED]

On January 12, 2018 a semi-weekly (Monday/Thursday) report, labeled [REDACTED] was implemented. This report tracks baselines that have control changes completed but configurations not updated. The report is sent via email to the Information Technology Managers and the Compliance Team.

Please see: [REDACTED]

Scope:

To determine scope of changes which did not include validation of CIP-005 and CIP-007 security controls during the testing of the change as per CIP-010-2 R1.5 a programmatic cross check was performed of

CIPv5 change controls impacting the CIP-010 R1.1 baseline of a CIP protected asset was performed. CIPv5 change controls referencing, as a testing predecessor, any change control from the CIPv3 queue or a CIPv5 change control designated as not impacting a CIP-010 baseline were flagged by this automated review.

To determine scope for CIP-010 baseline not updated within 30 days as per CIP-010-2 R1.3, in addition to the PCAs documented during the initial discovery, a manual review of change controls was conducted and checked against the documentation updates to the CIP-010 R1.1 lists in EMS SharePoint. Additionally, non-compliant configuration items were checked against open change controls and remediation tickets. No additional findings during review.

To determine scope for unmonitored hotfix and security patch baselines as per CIP-010 R1.1, in addition to the EACMs and EAPs documented during initial discover, a Compliance security analyst work with the network engineers to ensure no other devices required additional baseline monitoring and/or documentation for CIP-010 R1.1 baselines. A manual review of review of CIPv5 change controls impacting CIP-010 baselines was conducted and crosschecked against baseline updates to determine if other changes impacting the CIP-010 baseline of a CIP protected asset was not reflected in monitoring tools and baseline documentation. No additional findings.

Root Cause: In each of the specified events above the root cause is directly related to a lack of a defined procedure or process for the designated task to be performed or completed. Additionally the absence of assignment of roles and responsibilities for completing the designated tasks was identified as contributing factor to the root cause.

Overall Mitigation: To minimize the risk of reoccurrence and ultimately strengthen internal documentation, created the Baseline Management Plan. The Baseline Management Plan was implemented on May 15, 2018 and consists of the Plan itself, policies and procedures, and job aides. Training was provided to all change control implementers prior to the Baseline Management Plan being implemented. Mitigation also included enhancements to oversight capabilities in way of streamlining the change control form into one form and adding baseline update monitoring and analyst review oversight to the Compliance Dashboard.

The following documents make up the Baseline Management Plan

1. [REDACTED]

Please see folder: [REDACTED]

Change control implementers were provided training on the Baseline Management Plan including the supporting documentation listed above by May 1, 2018.

Training provided can be reviewed here, please see:

1. [REDACTED]

Training was held on three different occasions, participation was mandatory and tracked, please see training invitations and attendance:

1. [REDACTED]

After the training [REDACTED] obtained signatures from the change control implementers that each individual read and understood the Baseline Management Plan and its associated documentations, please see folder:

1. [REDACTED]

Additionally, [REDACTED] added two oversight capabilities:

1. Merging the change control form into one form places a control in-between the testing and implementation to production phase. Secondly it streamlines the process for the change control implementer and makes oversight of the ticket more efficient. This was completed with the implementation of the Baseline Management Plan on 5/15/2018.

- a. Please see: [REDACTED]

2. The original report, [REDACTED], was enhanced by creating two reports. The first report tracks baselines that need updating after the work has been completed and the second report tracks the Compliance Security Analyst review of the updated baselines. These two reports were implemented along with the Baseline Management Plan. Both reports were emailed daily until the Compliance Dashboard on SharePoint was updated. The updated occurred on 8/20/2018, following this the reports are emailed out bi-weekly (Monday and Thursdays)

Please see:

- a. [REDACTED]

The details of the [REDACTED] reports can be found in the Change Control and Configuration Management Policy.

Please see: [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: November 20, 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
Updating Baselines	[REDACTED]	12/27/2017	12/27/2017	Work was completed on 12/15/2017, final review completed on 12/27/2017.	No
Develop baseline and configuration monitoring	Development of [REDACTED] and [REDACTED] baselines configurations and configuring [REDACTED] to monitor applied	03/27/2018	03/27/2018		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
	security patches				
Confirmation of Scope	Scope was confirmed	04/15/2018	04/15/2018		No
Baseline Management Plan	Developed Baseline Management Plan and associated documents. Training to be provided to the change control implementers before the Baseline Management Plan goes into effect on 5/15/2018.	05/01/2018	05/01/2018		No
Creation CIP-010 reports	Two reports were created, one to track baselines that need updating after the work has been completed and the second report tracks the Compliance Security Analyst review of the updated baselines. These reports are emailed daily.	05/15/2018	05/15/2018		No
Single change control form	Merged the change control form into one form for testing and implementation to production phase	05/15/2018	05/15/2018		No
Employee Acknowledgement	Obtain individuals employee signatures acknowledging review of the Baseline Management Plan and associated documents.	07/02/2018	07/02/2018		No
Update Compliance Dashboard on SharePoint	Update the compliance dashboard with the two new CIP-010 reports: [REDACTED]	08/20/2018	08/20/2018		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
	[REDACTED]				
Validation for CIP-005-5 R1.5 for assets in testing	Change control remediation document for CIP-010 R1.5.1 and 1.5.2, validation of the security control for CIP-005-5 R1.5  See: [REDACTED]	11/20/2018	11/20/2018		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.

The risk to the reliability BES was minimal during the implementation of the mitigation plan.

While additional internal controls were required to ensure the proper documentation of changes to asset baselines the core CIP-005 and CIP-007 security controls were not impacted.

Network segmentation, traffic monitoring, logging, and the detection of malicious code were working as expected during and prior to the implementation of this mitigation plan.

### 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

This mitigation prevents recurrence of potential noncompliance by establishing and implementing a process with defined responsibilities.

Consolidating the testing and production implementation stages into a single change control prevents recurrence by streamlining oversight of the testing process and accommodates additional automated content validation.

The automated email reporting and the Compliance Dashboard reduce the risk of recurrence by improving visibility into the change control process and facilitating oversight by IT managers and the compliance department.

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.

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

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

Authorized Individual

Name: ██████████

Title: Manager of Compliance

Authorized On: November 27, 2018

Attachment 3

3c. The Entity's Certification of Mitigation  
Completion for CIP-010-2 R1 Part 1.5 submitted  
on November 27, 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): WECC2018019192

Mitigated Standard Requirement(s): CIP-010-2 R1.

Scheduled Completion as per Accepted Mitigation Plan: November 20, 2018

Date Mitigation Plan completed: November 20, 2018

WECC Notified of Completion on Date: November 27, 2018

Entity Comment:

Additional Comments		
From	Comment	User Name
Entity	Milestone Updating Baselines: [REDACTED]	[REDACTED]
Entity	Milestone Validation for CIP-005-5 R1.5 for assets in testing: Reference [REDACTED]	[REDACTED]
Entity	Milestone Develop baseline and configuration monitoring: [REDACTED] [REDACTED] [REDACTED]	[REDACTED]
Entity	Milestone Confirmation of Scope: Reference "WECC2018019192_Scope_Attestation.pdf" and folder "Production and Testing Change Control Pdfs.zip"	[REDACTED]
Entity	Milestone Baseline Management Plan Developed (includes training to employees): Reference 1. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]
Entity	Milestone Single change control form: Reference [REDACTED]	[REDACTED]
Entity	Milestone Creation CIP-010 Reports: Reference [REDACTED] [REDACTED]	[REDACTED]

Additional Comments		
From	Comment	User Name
Entity	[REDACTED]	[REDACTED]
Entity	Milestone Employee Acknowledgement Obtained: Reference Folder [REDACTED] [REDACTED]	[REDACTED]
Entity	Milestone Update Compliance Dashboard on SharePoint: [REDACTED] [REDACTED]	[REDACTED]

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED] [REDACTED]	Folder contains [REDACTED] individual change control .pdf's for the validation evidence	11,740,937
Entity	[REDACTED]	Creation [REDACTED] baseline	70,401
Entity	[REDACTED]	[REDACTED] configured to monitor [REDACTED] applied security patches	88,345
Entity	[REDACTED]	Creation [REDACTED] Baseline	128,705
Entity	[REDACTED]	[REDACTED] configured to monitor [REDACTED] applied security patches	102,378
Entity	[REDACTED]	Baseline creations for 12-15-2017 instances	427,018
Entity	[REDACTED] [REDACTED]	Implementation of the "Completed CIP-010 Changes" report	42,654
Entity	[REDACTED] [REDACTED]	Folder containing Baseline Management Plan and associated documents	5,310,987
Entity	[REDACTED] [REDACTED]	Baseline Management Plan Training Presentation	191,250
Entity	[REDACTED] [REDACTED]	Training meeting invitation 4.24.2018	137,216
Entity	[REDACTED] [REDACTED]	Training meeting invitation 4.26.2018	113,664
Entity	[REDACTED] [REDACTED]	Training meeting invitation 4.30.2018	79,872
Entity	[REDACTED] [REDACTED]	Network department training attendance	10,306
Entity	[REDACTED] [REDACTED]	System Administration department training attendance	10,404
Entity	[REDACTED] [REDACTED]	Applications department training attendance	10,489
Entity	[REDACTED] [REDACTED]	Employee certificates for class date 4.24.2018	885,290
Entity	[REDACTED] [REDACTED]	Employee certificates for class date 4.26.2018	402,004

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED]	Employee certificates for class date 4.30.2018	312,734
Entity	[REDACTED]	Folder contains individual employee signatures for acknowledgement and review of the Baseline Management Plan and associated documentation	1,992,798
Entity	[REDACTED]	Example of the merged change control into one ticket, combining the test and production phases	360,217
Entity	[REDACTED]	New Report tracking Baseline Updates required	38,323
Entity	[REDACTED]	New report tracking Compliance Security Analyst reviews required	38,311
Entity	[REDACTED]	New oversight reports added to the compliance dashboard on SharePoint	81,364
Entity	[REDACTED]	Change Control remediation document for CIP-010 R1.5.1 and 1.5.2 as pertaining to the validation of the security control established by CIP-005-5 R1.5. See pdf comments for additional information.	1,801,017
Entity	[REDACTED]	Attestation for confirming scope	110,226

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: Manager of Compliance  
 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. Verification of Mitigation Plan Completion  
for CIP-010-2 R1 Part 1.5 dated January 8, 2019

From: noreply@oati.net

Sent:

To: [REDACTED]

Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 R1. - [REDACTED]

---

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

**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](mailto:support@oati.net).**

NERC Registration ID: [REDACTED]  
NERC Violation ID: WECC2018019192  
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 11/27/2018 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>

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

[OATI Information - Email Template: MitPlan\_Completed]

Attachment 3

3e. The Entity's Self-Report of violation of  
CIP-010-2 R1 Part 1.1 submitted October 12, 2017

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-010-2

Requirement: CIP-010-2 R1.

Date Submitted: October 12, 2017

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: July 01, 2016

End/Expected End Date: June 01, 2017

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [REDACTED]. As defined in NERC Reliability Standard CIP-010-2, Requirement 1, Part 1.1 [REDACTED] is required to develop baseline configurations, individually or by a group, which shall include (Requirement 1.1.1): Operating system(s) (including version) or firmware where no independent operating system exists. Further, as defined in Requirement 2, Part 2.1, [REDACTED] is required to monitor at least once every 35 calendar days for changes to baseline configurations as described in NERC Requirement 1, Part 1.1. [REDACTED] is also required to document and investigate detected unauthorized changes per Requirement 2, Part 2.1.

On August 15, 2017, [REDACTED] discovered Sharepoint email reminder workflows were stalled and began manual reviews. The Sharepoint workflows stalled during a Sharepoint version upgrade. All reviews were completed within the 35 day monitoring deadline with the exception of a Polycom (video conferencing used within [REDACTED] control rooms) manual baseline. This review was completed on August 15, 2017. No baseline changes were identified but the review was 22 days past the 35 day deadline for monitoring.

In accordance with [REDACTED] Internal Compliance Program:

1. The Information Technology Department notified the Compliance department of the potential violation.
2. The Compliance team reviewed the event, determined a potential violation existed and convened [REDACTED] Compliance Committee.
3. The Compliance Committee agreed that a potential violation existed and a self-report was warranted. In addition, [REDACTED] Compliance team began a review of [REDACTED] approach to facilitation of Compliance with NERC Reliability

## Self Report

Standard CIP-010-2. Part of this review was a request to the Information Technology department to perform a review of all baseline configurations and workflows.

On September 28, 2017, in accordance with [REDACTED] Internal Compliance Program:

1. The Information Technology department notified the Compliance department of an event which may have resulted in two potential violations of NERC Reliability Standard CIP-010-2. On June 1, 2017, [REDACTED] developed baseline configurations for several [REDACTED] servers [REDACTED] which hadn't been in place since the effective date of NERC Reliability Standard CIP-010-2 (July 1, 2016). (CIP-010-2, Requirement 1.1.1) In addition, [REDACTED] didn't monitor this baseline configuration as required by CIP-010-2, Part 2.1 within 35 days. Manual review occurred on July 10, 2017.
2. On October 3, 2017, the Compliance team completed review of the June 1/July 10 events, determined potential violations existed and convened [REDACTED] Compliance Committee.
3. On October 12, 2017, the Compliance Committee agreed that potential violations existed and a self-report was warranted.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: As part of [REDACTED] ongoing effort to identify, evaluate, validate, monitor and test internal controls per [REDACTED] Internal Control Procedure, [REDACTED] will continue full evaluation of CIP-010-2 controls and notify WECC when that evaluation is complete by no later than November 17, 2017.

Immediate mitigation has taken place through performance of manual reviews. Mitigation underway but not completed at this time includes the following:

1. Compliance Workflow List - A compliance workflow list will be created to identify all automatic and manual workflows. This list will be sent to all Information Technology Managers [REDACTED] and the Compliance team twice weekly via email. The list will show: the workflow (automatic or manual), primary and secondary positions responsible for the workflow review and the number of days until the workflow review must be completed. Creation of this control will prevent additional issues should automated Sharepoint workflows fail in the future. This control as well as roles and responsibilities will be documented within [REDACTED] Change Control and Configuration Management process. The Information Technology and Compliance teams will review the list during our monthly IT-Compliance team touchpoint meetings. The workflow list and process revision mitigation will be completed by November 17, 2017.
2. Change Control and Configuration Management training - Training will be provided to all employees with roles relating to the process. This mitigation will be completed by November 17, 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: Minimal because:

1. Although the [REDACTED] server's baseline configuration hadn't been developed, [REDACTED] servers were having automatic patch checks performed and no changes were identified during the period of time in question.
2. Review of the [REDACTED] servers on July 10, 2017 identified no changes to the baseline configuration.
3. No baseline changes were identified for the Polycom manual baseline. No actual impact.

Self Report

Risk Assessment of Impact to Risk was minimal as no changes were identified.  
BPS:

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 3

3f. The Entity's Mitigation Plan designated as  
WECCMIT014184 for CIP-010-2 R1 Part 1.1  
submitted October 5, 2018



## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: WECCMIT014184

Mitigation Plan Version: 1

<u>NERC Violation ID</u>	<u>Requirement</u>	<u>Violation Validated On</u>
WECC2017018484	CIP-010-2 R1.	01/29/2018

Mitigation Plan Submitted On: October 05, 2018

Mitigation Plan Accepted On: November 15, 2018

Mitigation Plan Proposed Completion Date: June 15, 2018

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On: November 07, 2018

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		
WECC2017018484	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:

On May 29, 2017, during the development of the [REDACTED] programmatic node validation it was determined that the [REDACTED] CIP-010 R1.1.1 baseline had not been documented or monitored in [REDACTED] Whitelist Profiler. On June 1, 2017, [REDACTED] developed baseline configurations for several [REDACTED] servers ([REDACTED]) which hadn't been in place since the effective date of NERC Reliability Standard CIP-010-2 (July 1, 2016). (CIP-010-2, Requirement 1.1.1)

On September 28, 2017, in accordance with [REDACTED] Internal Compliance Program, the Information Technology department notified the Compliance department of an event which may have resulted in a potential violation of NERC Reliability Standard CIP-010-2.

On October 3, 2017, the Compliance team completed review of the June 1 findings and determined a potential violation existed and convened [REDACTED] Compliance Committee.

On October 12, 2017, the Compliance Committee agreed that potential violations existed and a self-report was warranted.

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

See above

## 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:

Discovery and Mitigation Timeline for the Cyber Assets in scope of Potential Noncompliance for CIP-010 R1

I. Discovery: Missing R1.1.1 CIP-010 baseline for the [REDACTED] Systems ([REDACTED] Cyber Assets)

May 29, 2017, during the development of the [REDACTED] programmatic node validation it was determined that the [REDACTED] CIP-010 R1.1.1 baseline had not been documented or monitored in [REDACTED] [REDACTED] [REDACTED]

II. Mitigation: Manual Baseline Checks Created

On June 1, 2017, manual baseline checks were created for the [REDACTED] systems in the Manual Baseline Review list. See [REDACTED]

III. Mitigation: Implementation of Asset Inventory Automation

On August 17th, 2017 automation of asset monitoring inventory assessment fully implemented. Ensures all CIP protected assets are present either in the Manual Baseline Tracking process or present in [REDACTED] for automated monitoring.

See: [REDACTED]

IV. Mitigation: Implementation of Automated Policy Assessment

On September 9th, 2017 automated policy assessment as part of the automated baseline import process for [REDACTED] policy creation fully automated. This process assess baselines, based on the criteria established by the root CIP-010-2 list, to ensure that all baselines have data present.

See [REDACTED]

V. Mitigation: Updated procedures to reflect new asset deployments

On June 16, 2018 a new version of the Change Control Procedure was made effective. The [REDACTED] [REDACTED] added language regarding new asset deployments.

Please see: [REDACTED]

Scope:

Completed September 9th 2018.

Scope was determined using the same automated checks which discovered the lack of documentation of the CIP-010-2 R1.1.1 baseline for the [REDACTED] systems. These checks were used to ensure the migration from [REDACTED] [REDACTED] was complete and no asset monitoring or documentation was not migrated.

See: [REDACTED] and [REDACTED]

No additional logical asset group or unique asset groups were found with undocumented CIP-010-2 R1.1 baselines.

Mitigation Summary:

During the implementation of [REDACTED] to replace [REDACTED] [REDACTED] [REDACTED] [REDACTED] a programmatic process was introduced to ensure that all assets within the scope of CIP and, where technically feasible, their test analogs were present in [REDACTED] if capable automated monitoring or present on the Manual Baseline Review SharePoint list.

See: [REDACTED] and [REDACTED]

For assets which could be automatically tracked, a programmatic process validates that baseline data exists for all CIP-010 R1.1 sub-requirements which are designated as required by the CIP-010 baseline list item for the logical asset group. The development of this process is what initially discovered the lack of a CIP-010 R1.1.1 baseline for the [REDACTED] Systems.

See [REDACTED]

**Root cause:**

The root cause of the failure to monitor assets can be segmented into two unique failures in process and internal controls.

Personnel did not have detailed processes to follow which resulted in an incorrect decision regarding documenting baselines for these devices along with steps that address remediation and mitigation.

Large volume of information requiring manual correlation was untenable. This led to the issue going undiscovered until the migration to [REDACTED] and the implementation of automated reviews for asset monitoring inventory and policy assessment.

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: June 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
Create Manual Baseline Checks	Manual baseline checks created.	06/01/2017	06/01/2017		No
Automate Asset Inventory	Implemented Asset Inventory automation	08/17/2017	08/17/2017		No
Node Validation Report	Automation of Node Validation Report	09/08/2017	09/08/2017		No
Document Update Proposals	Initial conversations for updating documentation and the early stages of conversation for the need of developing and overarching plan. Later known as the Baseline Management Plan	12/07/2017	12/07/2017		No
Drafting Baseline Management Plan	Initial draft versions of the Baseline Management Plan and associated documents, including "Change Control	03/09/2018	03/09/2018		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
	Procedure.				
Change Control Procedure	Change Control Procedure updated to include new section regarding new asset deployments. Procedure was updated on 5/30/2018 and went effective 6/15/2018.	05/30/2018	05/30/2018		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.

The risk to the reliability BES was minimal during the implementation of the mitigation plan. Workflows during this time were monitored for failure. Additionally there was not impact to the CIP-005 and CIP-007 security controls used to secure the systems.

### Prevention

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

This mitigation prevents recurrence of potential noncompliance by establishing roles and responsibilities for the implementation and monitoring of systems which are members of new logical asset group. Automation implemented to audit asset inventory and assess applied [REDACTED] policies from CIP-010-2 R1.1 baselines improves oversight of baseline documentation to reduce the risk of documentation gaps.

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.

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

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

Authorized Individual

Name: ██████████

Title: ████████████████████

Authorized On: October 05, 2018

Attachment 3

3g. The Entity's Certification of Mitigation  
Completion for CIP-010-2 R1 Part 1.1 dated  
November 7, 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): WECC2017018484

Mitigated Standard Requirement(s): CIP-010-2 R1.

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

Date Mitigation Plan completed: June 15, 2018

WECC Notified of Completion on Date: November 07, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED]	Change Control Procedure	871,477
Entity	[REDACTED]	Automated policy assessment, part of the automated baseline import process for [REDACTED]	234,556
Entity	[REDACTED]	Manual baseline checks created for [REDACTED] servers.	160,573
Entity	[REDACTED]	Automation of asset monitoring inventory assessment fully implemented.	410,726

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: Manager of Compliance

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

3h. Verification of Mitigation Plan Completion for  
CIP-010-2 R1 Part 1.1 dated August 6, 2019

From: noreply@oati.net

Sent:

To: [REDACTED]

Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 R1. - [REDACTED]

---

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

**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: WECC2017018484  
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 11/07/2018 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>

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

[OATI Information - Email Template: MitPlan\_Completed]

## Attachment 4

4a. The Entity's Self-Report of violation of  
CIP-010-2 R2 Part 2.1 submitted October 12, 2017

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-010-2

Requirement: CIP-010-2 R2.

Date Submitted: October 12, 2017

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: June 01, 2017

End/Expected End Date: July 10, 2017

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [REDACTED]. As defined in NERC Reliability Standard CIP-010-2, Requirement 1, Part 1.1 [REDACTED] is required to develop baseline configurations, individually or by a group, which shall include (Requirement 1.1.1): Operating system(s) (including version) or firmware where no independent operating system exists. Further, as defined in Requirement 2, Part 2.1, [REDACTED] is required to monitor at least once every 35 calendar days for changes to baseline configurations as described in NERC Requirement 1, Part 1.1. [REDACTED] is also required to document and investigate detected unauthorized changes per Requirement 2, Part 2.1. On August 15, 2017, [REDACTED] discovered Sharepoint email reminder workflows were stalled and began manual reviews. The Sharepoint workflows stalled during a Sharepoint version upgrade. All reviews were completed within the 35 day monitoring deadline with the exception of a Polycom (video conferencing used within [REDACTED] control rooms) manual baseline. This review was completed on August 15, 2017. No baseline changes were identified but the review was 22 days past the 35 day deadline for monitoring. In accordance with [REDACTED] Internal Compliance Program:  
1. The Information Technology Department notified the Compliance department of the potential violation.  
2. The Compliance team reviewed the event, determined a potential violation existed and convened [REDACTED] Compliance Committee.  
3. The Compliance Committee agreed that a potential violation existed and a self-report was warranted. In addition, [REDACTED] Compliance team began a review of [REDACTED] approach to facilitation of Compliance with NERC Reliability Standard CIP-010-2. Part of this review was a request to the Information



## Self Report

Technology department to perform a review of all baseline configurations and workflows.

On September 28, 2017, in accordance with [REDACTED] Internal Compliance Program:

1. The Information Technology department notified the Compliance department of an event which may have resulted in [REDACTED] potential violations of NERC Reliability Standard CIP-010-2. On June 1, 2017, [REDACTED] developed baseline configurations for several [REDACTED] servers ([REDACTED]) which hadn't been in place since the effective date of NERC Reliability Standard CIP-010-2 (July 1, 2016). (CIP-010-2, Requirement 1.1.1) In addition, [REDACTED] didn't monitor this baseline configuration as required by CIP-010-2, Part 2.1 within 35 days. Manually review occurred on July 10, 2017.

2. On October 3, 2017, the Compliance team completed review of the June 1/July 10 events, determined potential violations existed and convened [REDACTED] Compliance Committee.

3. On October 12, 2017, the Compliance Committee agreed that potential violations existed and a self-report was warranted.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: As part of [REDACTED] ongoing effort to identify, evaluate, validate, monitor and test internal controls per [REDACTED] Internal Control Procedure, [REDACTED] will continue full evaluation of CIP-010-2 controls and notify WECC when that evaluation is complete by no later than November 17, 2017.

Immediate mitigation has taken place through performance of manual reviews.

Mitigation underway but not completed at this time includes the following:

1. Compliance Workflow List - A compliance workflow list will be created to identify all automatic and manual workflows. This list will be sent to all Information Technology Mangers (3) and the Compliance team twice weekly via email. The list will show: the workflow (automatic or manual), primary and secondary positions responsible for the workflow review and the number of days until the workflow review must be completed. Creation of this control will prevent additional issues should automated Sharepoint workflows fail in the future. This control as well as roles and responsibilities will be documented within [REDACTED] Change Control and Configuration Management process. The Information Technology and Compliance teams will review the list during our monthly IT-Compliance team touchpoint meetings. The workflow list and process revision mitigation will be completed by November 17, 2017.
2. Change Control and Configuration Management training - Training will be provided to all employees with roles relating to the process. This mitigation will be completed by November 17, 2017.

Have Mitigating Activities No  
been Completed?

Date Mitigating Activities  
Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Actual Impact to BPS: Minimal because:

1. Although the [REDACTED] server's baseline configuration hadn't been developed, [REDACTED] servers were having automatic patch checks performed and no changes were identified during the period of time in question.
2. Review of the [REDACTED] servers on July 10, 2017 identified no changes to the baseline configuration.
3. No baseline changes were identified for the Polycom manual baseline. No actual impact.

Self Report

Risk Assessment of Impact to Risk was minimal as no changes were identified.  
BPS:

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  
WECCMIT013978-2 for CIP-010-2 R2 Part 2.1  
submitted August 30, 2018

## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: WECCMIT013978-2

Mitigation Plan Version: 3

NERC Violation ID	Requirement	Violation Validated On
WECC2017018485	CIP-010-2 R2.	06/14/2018

Mitigation Plan Submitted On: August 30, 2018

Mitigation Plan Accepted On: September 04, 2018

Mitigation Plan Proposed Completion Date: December 11, 2017

Actual Completion Date of Mitigation Plan:

Mitigation Plan Certified Complete by [REDACTED] On: September 07, 2018

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		
WECC2017018485	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:

On August 15, 2017 [REDACTED] discovered Sharepoint email reminder workflows were stalled and began manual reviews. The Sharepoint workflows stalled during a Sharepoint version upgrade. All reviews were completed within the 35 day monitoring deadline with the exception of a Polycom (video conferencing used within [REDACTED] control rooms) manual baseline. This review was completed on August 15, 2017. No baseline changes were identified but the review was 22 days past the 35 day deadline for monitoring.

In accordance with [REDACTED] Internal Compliance Program:

1. The Information Technology Department notified the Compliance department of the potential violation.
2. The Compliance team reviewed the event, determined a potential violation existed and convened [REDACTED] Compliance Committee.
3. The Compliance Committee agreed that a potential violation existed and a self-report was warranted. In addition, [REDACTED] Compliance team began a review of [REDACTED] approach to facilitation of Compliance with NERC Reliability Standard CIP-010-2. Part of this review was a request to the Information Technology department to perform a review of all baseline configurations and workflows.

On September 28, 2017, in accordance with [REDACTED] Internal Compliance Program:

1. The Information Technology department notified the Compliance department of an event which may have resulted in two potential violations of NERC Reliability Standard CIP-010-2. On June 1, 2017, [REDACTED] developed baseline configurations for several [REDACTED] servers ([REDACTED]) which hadn't been in place since the effective date of NERC Reliability Standard CIP-010-2 (July 1, 2016). (CIP-010-2, Requirement 1.1.1) In addition, [REDACTED] didn't monitor this baseline configuration as required by CIP-010-2, Part 2.1 within 35 days. Manually review occurred on July 10, 2017.
2. On October 3, 2017, the Compliance team completed review of the June 1/July 10 events, determined potential violations existed and convened [REDACTED] Compliance Committee.
3. On October 12, 2017, the Compliance Committee agreed that potential violations existed and a self-report was warranted.

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

See summary.

## 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:

Discovery and Mitigation Timeline for the [REDACTED] Cyber Assets in scope of Potential Noncompliance for CIP-010 R2

I. Discovery: Missing R1.1.1 CIP-010 baseline for the [REDACTED] Systems ([REDACTED] Cyber Assets)  
May 29, 2017, during the development of the [REDACTED] programmatic node validation it was determined that the [REDACTED] CIP-010 R1.1.1 baseline had not been documented or monitored in [REDACTED] [REDACTED] [REDACTED]

II. Mitigation: Manual Baseline Checks Created

On June 1, 2017, manual baseline checks were created for the [REDACTED] systems in the Manual Baseline Review list.

Root Cause:

Lack of clear process hampered oversight of the CIPv5 implementation of [REDACTED] [REDACTED] [REDACTED] [REDACTED] and Policy based baseline monitoring which led to a failure to properly evaluate and document CIP-010 R1.1 baseline sub-requirement and, therefore, the strategy to monitor them.

III. Discovery: Failed to Monitor the Baseline within 35 Days for Unauthorized Changes

On July 8, 2017, while working on programmatic validation of the Manual Baseline Check List a Compliance Security Analyst discovered that the [REDACTED] systems were not checked. Email sent system administrations to perform baseline review.

IV. Mitigation: System Baselines for [REDACTED] Systems Performed

On July 10, 2017, baseline review of the [REDACTED] Systems were conducted by the patch check owner.

Root Cause:

Initial check had not been entered into the Baseline Review Log. Because of this, the SharePoint workflow responsible for notifying responsible parties did not function properly and failed to notify the responsible parties to review the baselines for the [REDACTED] systems.

Mitigation Summary:

During the implementation of [REDACTED] to replace [REDACTED] [REDACTED] [REDACTED] [REDACTED] a programmatic process was introduced to ensure that all assets within the scope of CIP and, where technically feasible, their test analogs were present in [REDACTED] if capable automated monitoring or present on the Manual Baseline Review SharePoint list.

For assets which could be automatically tracked, a programmatic process validates that baseline data exists for all CIP-010 R1.1 sub-requirements which are designated as required by the CIP-010 baseline list item for the logical asset group. The development of this process is what initially discovered the lack of a CIP-010 R1.1.1 baseline for the [REDACTED] Systems.

V. Discovery: No Baseline Review for [REDACTED] Polycom System ([REDACTED] Cyber Assets)

On August 8, 2017, the SharePoint team discovered an issue with the Manual Baseline Review automated workflows and corrected it. This generated an email notify compliance and the responsible party that a patch check had not been performed for the [REDACTED] Polycom System.

On August 15th, 2018 the review of the [REDACTED] PCA's baselines was completed and migration was completed.

VI. Mitigation: Automation of Node Validation Report

On August 17, 2017, Report automating the cross check of [REDACTED] node membership, the Cyber Asset



List, and the Manual Baseline Review list create. [REDACTED] policy creation automation deployed. Automation ensures that all CIP-Protected assets monitored by [REDACTED] or manually are present and that CIP-010 R1.1 baselines are documented in EMS SharePoint.

VII. Mitigation: Implementation of Compliance Dashboard

On November 13, 2017, Compliance Dashboard and email reports implemented to monitor the status of Manual Baseline Review due dates, Mitigation Plan due dates, and Security Patch Review due dates.

VIII. Mitigation: Training Issued to Staff for Manual Baseline Tracking

On December 11, 2017, training was completed by staff and test results collected for the Manual Baseline Tracking System.

Root Cause:

The reliance on SharePoint workflow driven notifications and no internal control to account or compensate for the failure of SharePoint workflow to notify responsible parties of upcoming baseline reviews.

Mitigation Summary:

The compliance dashboard was created in SharePoint to provide the Compliance Department and IT manager's real time information regarding the status of Manual Baseline Reviews, Security Patch Reviews, and Mitigation plans. Entries are color coded based and ascendingly sorted based on the number of days that have passed since the last review.

The timestamp used in conjunction with the current system time to create the days past metric is created using a SharePoint workflow. However, the color coding evaluation and sorting tasks are performed using JavaScript and SharePoint features independent of workflow functionality. In the event a workflow fails and the date reviewed is not updated, the impacted assets position in the list and color coding will not be impacted. This improves resilience by providing visibility into the upcoming due date's independent of notification workflow functionality.

Automated email is sent out every Monday and Thursday which contains the last review date for Manual Baseline Reviews, Security Patch Reviews, and Mitigation plans.

The dashboard and report email are reviewed by the Compliance Department and IT managers to ensure that all checks occur within the timeframes set forth by the NERC CIP Reliability Standards.

The scheduling and creation of this report is orchestrated using [REDACTED]. This improves the resilience of the notification system as the failure of SharePoint workflows has no impact on the behavior of the Compliance Report email. This provides an internal control which will prevent recurrence of potential non-compliance related to the failure of SharePoint Workflows.

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: December 11, 2017

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

Milestone Activity	Description	*Proposed Completion Date (Shall not be greater than 3 months apart)	Actual Completion Date	Entity Comment on Milestone Completion	Extension Request Pending

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
Create Manual Baseline Checks	[REDACTED] [REDACTED] [REDACTED] [REDACTED]	06/01/2017	06/01/2017		No
Perform System Baselines for [REDACTED] Systems	Patch Check Owner to conduct baseline review of the [REDACTED] Systems.	07/10/2017	07/10/2017		No
Perform Baseline Review	Completed the manual baseline review for the PolyCom systems, no baseline changes were identified.	08/15/2017	08/15/2017	No baseline changes were identified.	No
Automate Node Validation Report	Create report automating the cross check of [REDACTED] node membership, the Cyber Asset List, and the Manual Baseline Review List. Deployed [REDACTED] Policy creation automation.	08/17/2017	08/17/2017		No
Develop and Implement Compliance Dashboard	Develop and implement a Compliance Dashboard and email reports to monitor the status of Manual Baseline Review due dates, Mitigation Plan due dates, and Security Patch Review due dates.	11/13/2017	11/13/2017		No
Manual Baseline Tracking Training	Develop and deliver Manual Baseline Tracking System training.	12/11/2017	12/11/2017		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.

The risk to the reliability BES was minimal during the implementation of the mitigation plan. Workflows during this time were monitored for failure. Additionally there was no impact to the CIP-005 and CIP-007 security controls used to secure the systems.

### Prevention

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

This mitigation prevents recurrence of potential noncompliance by establishing roles and responsibilities for the implementation and monitoring of systems which are members of new logical asset group. Further, the Compliance Dashboard and the Compliance Report emails and the review process ensure that SharePoint workflow failures are detected prior to an instance of potential noncompliance.

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

In addition to internal controls which detect the failure of SharePoint workflows and prevent the omission of baseline data, [REDACTED] has developed the Baseline Management Plan to comprehensively mitigate CIP-010 compliance risk. This is supplemented by a robust set of automated auditing capabilities to ensure that all systems under the scope of CIP are monitored for baseline data at least once every 35 days which have been developed and implemented since the time of the initial self-report.

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.

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

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

Authorized Individual

Name: ██████████

Title: ████████████████████

Authorized On: July 13, 2018

Attachment 4

4c. The Entity's Certification of Mitigation Plan

Completion for CIP-010-2 R2 Part 2.1 dated

September 7, 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): WECC2017018485

Mitigated Standard Requirement(s): CIP-010-2 R2.

Scheduled Completion as per Accepted Mitigation Plan: December 11, 2017

Date Mitigation Plan completed: December 11, 2017

WECC Notified of Completion on Date: September 07, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED]	CIP-010 Mitigation Training PPT	234,582
Entity	[REDACTED]	CIP-010 Mitigation Training Quiz	36,652
Entity	[REDACTED]	CIP-010 Mitigation Training Certificates	789,000
Entity	[REDACTED]	Compliance Report Email Notification	35,144
Entity	compliance dashboard.PNG	Compliance Dashboard screen shot	256,646
Entity	[REDACTED]	Compliance Workflow Narrative	204,066
Entity	[REDACTED]	Compliance-IT Touchpoint Meeting Minutes	74,199
Entity	[REDACTED]		76,364
Entity	[REDACTED]		410,726

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

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

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

Attachment 4

4d. Verification of Mitigation Plan Completion for  
CIP-010-2 R2 Part 2.1 dated September 20, 2018



From: noreply@oati.net

Sent:

To: [REDACTED]

Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 R2. - [REDACTED]

---

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

**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: WECC2017018485  
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 09/07/2018 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>

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

[OATI Information - Email Template: MitPlan\_Completed]

Attachment 4

4e. The Entity's Self-Report of Violation of  
CIP-010-2 R2 submitted January 19, 2018

Self Report

Entity Name: [REDACTED]

NERC ID: [REDACTED]

Standard: CIP-010-2

Requirement: CIP-010-2 R2.

Date Submitted: January 19, 2018

Has this violation previously No  
been reported or discovered?:

Entity Information:

Joint Registration  
Organization (JRO) ID:

Coordinated Functional  
Registration (CFR) ID:

Contact Name: [REDACTED]

Contact Phone: [REDACTED]

Contact Email: [REDACTED]

Violation:

Violation Start Date: February 06, 2017

End/Expected End Date: January 15, 2018

Reliability Functions: [REDACTED]

Is Possible Violation still No  
occurring?:

Number of Instances: 1

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

Which Regions:

Date Reported to Regions:

Detailed Description and Cause of Possible Violation: [REDACTED] is required, as defined in NERC Reliability Standard CIP-010-2, Requirement 2, Part 2.1 to monitor for changes to baseline configuration every 35 days.

On January 15, 2018, during a Cyber Asset list review, [REDACTED] discovered that an [REDACTED] workstation monitored in [REDACTED] had been inadvertently set to "inactive" on September 29, 2017. Initial review revealed that the workstation hadn't been monitored for changes to logically accessible ports and services since February 6, 2017. An immediate review of all assets monitored in [REDACTED] was performed on January 15, 2018. The review revealed an additional [REDACTED] "active" [REDACTED] workstations had not been monitored since February 6, 2017 but their baselines were found to be in configuration. The [REDACTED] workstation baseline configurations weren't monitored as required due to an omission of the assets from the [REDACTED] asset list, which is manually populated.

Mitigating Activities:

Description of Mitigating Activities and Preventative Measure: Mitigation actions completed:  
1. Reviewed all [REDACTED] assets and baselines were found to be in configuration

Mitigation actions to be completed:  
1. Develop and implement a preventative control in the form of an automated

## Self Report

process to export assets monitored by [REDACTED] to prevent recurrence.

a. To be completed by January 26, 2018.

2. Develop and implement a preventative control in the form of an automated process to validate all assets requiring [REDACTED] monitoring via weekly scan.

a. To be completed by February 9, 2018.

3. Transfer monitoring of all assets in [REDACTED] to [REDACTED] which will allow for automated asset validation. This will ensure controls developed and implemented for other CIP-010 mitigation actions are taken advantage of for this issue as well. (e.g. Compliance Workflow Report)

a. To be completed by May 1, 2018. (Dependent on pending vendor upgrade)

Have Mitigating Activities No  
been Completed?

Date Mitigating Activities  
Completed:

Impact and Risk Assessment:

Potential Impact to BPS: Minimal

Actual Impact to BPS: Minimal

Description of Potential and Current baseline configurations were identical to baseline configurations in  
Actual Impact to BPS: February of 2016.

Risk Assessment of Impact to Current baseline configurations were identical to baseline configurations in  
BPS: February of 2016.

Additional Entity Comments:

Additional Comments		
From	Comment	User Name
No Comments		

Additional Documents			
From	Document Name	Description	Size in Bytes
No Documents			

Attachment 4

4f. The Entity's Mitigation Plan designated as  
WECCMIT014094 for CIP-010-2 R2 submitted

August 31, 2018

## Mitigation Plan

### Mitigation Plan Summary

Registered Entity: [REDACTED]

Mitigation Plan Code: WECCMIT014094

Mitigation Plan Version: 1

<u>NERC Violation ID</u>	<u>Requirement</u>	<u>Violation Validated On</u>
WECC2018019012	CIP-010-2 R2.	08/28/2018

Mitigation Plan Submitted On: August 31, 2018

Mitigation Plan Accepted On: November 13, 2018

Mitigation Plan Proposed Completion Date: February 20, 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: Manager of Compliance

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		
WECC2018019012	03/14/2017	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:

On January 15, 2018, during a Cyber Asset list review, [REDACTED] discovered an [REDACTED] workstation monitored in [REDACTED] had been inadvertently set to "inactive" on September 29, 2017. Initial review revealed that the workstation hadn't been monitored for changes to logically accessible ports and services since February 6, 2017. An immediate review of all assets monitored in [REDACTED] was performed on January 15, 2018. The review identified an additional [REDACTED] "active" [REDACTED] workstations which had not been monitored since February 6, 2017. However, their baselines were found to be in configuration. The [REDACTED] workstation baseline configurations weren't monitored as required due to an omission of the assets from the [REDACTED] asset list, which at the time was manually populated.

In accordance with [REDACTED] Internal Compliance Program:

1. The Security Analyst notified the Director of Compliance of the potential violation.
2. The Compliance team reviewed the event, determined a potential violation existed and convened [REDACTED] Compliance Committee.
3. The Compliance Committee agreed that a potential violation existed and a self-report was warranted. In addition, [REDACTED] Compliance team began a review of [REDACTED] approach to facilitation of Compliance with NERC Reliability Standard CIP-010-2. Part of this review was a request to the Information Technology department to perform a review of all baseline configurations and workflows.

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

See summary above.

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:

Discovery: [REDACTED] Media Consoles Not Reviewed for Unauthorized Changes.  
 On January 15, 2017, it was discovered that the [REDACTED] Media Consoles were not reviewed for unauthorized changes to the CIP-010 R1.1.4 baseline since February 6, 2017.

I. Mitigation: Review of the [REDACTED] Media Consoles.  
 On January 15, 2018, the [REDACTED] cyber assets were evaluated for logically accessible ports and services; no unauthorized changes to the baseline were discovered during this review.

II. Mitigation: Determine Scope.  
 On January 16, 2018, the scope was verified by the list of scanned IP from the [REDACTED] sites was manually crosschecked against the Cyber Asset List to ensure that all assets with baselines are monitored for unauthorized changes to the logically accessible ports and services baseline were scanned by [REDACTED]. No additional assets identified.

III. Mitigation: Creation of Cyber Asset Inventory [REDACTED] Site Population Script.  
 On February 1, 2018, script to programmatically generate a list of IP address for assets scanned by [REDACTED] from the Cyber Asset List was created and provided to the Compliance Security Analyst responsible for managing the port monitoring scans performed using [REDACTED].

IV. Mitigation: [REDACTED] Asset Validation.  
 On February 18, 2018, an automated reconciliation of assets scanned by [REDACTED] was implemented to verify that all assets requiring [REDACTED] scans had successfully been scanned within the last 72 hours using the [REDACTED] [REDACTED] logs. Validation is automated to run weekly.

Root cause:  
 The [REDACTED] [REDACTED] Workstation Consoles were omitted as a clerical error by a Compliance Security Analyst. Absence from the nightly scans continued due to a lack of oversight with the scan population process.

Mitigation Summary:  
 Automation of the [REDACTED] [REDACTED] scan site population asset selection process eliminates the opportunity for clerical errors by a Compliance Security Analyst while designating monitored assets. Validation of the [REDACTED] [REDACTED] scan engine log against the Cyber Asset List provides oversight by notifying the Compliance Department if CIP Protected assets are missing from the [REDACTED] Scan.

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: February 20, 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
Review [REDACTED] Media Consoles	Evaluate the [REDACTED] assets for logically	01/15/2018	01/15/2018	No findings.	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
	accessible ports and services. No unauthorized changes to the baseline were discovered during this review.				
Verified Scope	Ensure that all assets with baselines monitored for unauthorized changes to the logically accessible ports and services baseline were scanned by [REDACTED]. No additional cyber assets identified.	01/16/2018	01/16/2018	No additional findings.	No
Create Scan Site Population Script for [REDACTED]	To address the root cause and prevention of recurrence [REDACTED] created a Cyber Asset Inventory [REDACTED] Site Population Script to programmatically generate a list of IP addresses for assets scanned by [REDACTED] from the Cyber Asset List created and provided to the Compliance Security Analyst responsible for managing the port monitoring scans performed using [REDACTED].	02/01/2018	02/01/2018		No
Create [REDACTED] Asset Validation	Develop and implement an automated reconciliation of assets scanned by [REDACTED] to verify that all assets	02/20/2018	02/20/2018		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
	requiring [REDACTED] scans are successfully scanned within the last 72 hours using the [REDACTED] Scan Engine logs.				

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.

The risk to the reliability BES was minimal during the implementation of the mitigation plan. Current baseline configurations were identical to the baseline configurations in February 2016. Additionally there was no impact to the CIP-005 and CIP-007 security controls used to secure the systems

### Prevention

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

This mitigation prevents recurrence of potential noncompliance by establishing and implementing a preventative control by automating the process of selecting assets for the [REDACTED] scan site population. Validation of scan engine logs ensures that un-scanned assets are reported to the Compliance Department to prevent further prolonged omissions of CIP-Protected assets from monitoring of logically accessible ports and services by [REDACTED]

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

No required additional actions identified at this time

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] [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: Manager of Compliance

Authorized On: August 31, 2018

## Attachment 4

4g. The Entity's Certification of Mitigation Plan Completion for  
CIP-010-2 R2 submitted November 27, 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): WECC2018019012

Mitigated Standard Requirement(s): CIP-010-2 R2.

Scheduled Completion as per Accepted Mitigation Plan: February 20, 2018

Date Mitigation Plan completed: February 20, 2018

WECC Notified of Completion on Date: November 27, 2018

Entity Comment:

Additional Documents			
From	Document Name	Description	Size in Bytes
Entity	[REDACTED]	Evidence showing review of [REDACTED] Media Consoles .	1,976,250
Entity	[REDACTED]	Evidence verifying scope.	893,001
Entity	[REDACTED]	Evidence showing creation of the [REDACTED] [REDACTED] Population Script	510,578
Entity	[REDACTED]	Evidence showing completion of [REDACTED] [REDACTED] Validation	173,300

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

Name: [REDACTED]

Title: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

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



Attachment 4

4h. Verification of Mitigation Plan Completion for  
CIP-010-2 R2 dated December 19, 2018

From: noreply@oati.net  
Sent: 12/12/2018 14:22:18  
To: [REDACTED]  
Subject: WECC Notice - Completed Mitigation Plan Acceptance - CIP-010-2 R2. - [REDACTED]

---

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

**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: WECC2018019012  
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 11/27/2018 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>

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

[OATI Information - Email Template: MitPlan\_Completed]