COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	WECC2016016686	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	WECC2017017207	Yes	Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
3	WECC2017016991			Yes	Yes							Yes		Category 2 – 12: 2 years
4	WECC2017017204			Yes	Yes						Yes			Category 2 – 12: 2 years
5	WECC2017017208	Yes	Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
6	WECC2017017206			Yes	Yes						Yes			Category 2 – 12: 2 years
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														
35														
36														

Filing Date: March 28, 2019

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2016016686	CIP-002-5.1	R1; P1.2	High	Lower	7/1/2016 (when the Standard became mandatory and enforceable)	5/11/2017 (Mitigation Plan completion)	Self-Report	5/11/2017	6/1/2017

Description of the Violation (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, or confirmed violation.)	On December 16, 2016, the entity submitted a Self-Report stating that, [redacted], it was in noncompliance with CIP-002-5.1 R1. Specifically, the entity reported it started its BES Asset analysis utilizing CIP Version 5 criteria in November 2014. The most comprehensive data sources for the entity's asset characteristics were identified and used to categorize the BES Assets. The first entity-approved CIP-002-5.1 BES Cyber System list was published May 12, 2015 to align with the entity's CIP Version 5 transition project. During the entity's November 2016 CIP-002-5.1 BES Cyber System review, a new preferential data source was identified and used to re-categorize the Low Impact Bulk Electric System (BES) Cyber Systems (LIBCS) at a substation to Medium Impact BES Cyber Systems (MIBCS). Upon evaluation of the change, it was determined that the BES Asset information used to initially categorize the LIBCS was unclear and incomplete which resulted in the incorrect impact rating for the BES Cyber Systems at that substation. The entity had categorized the BES Cyber System at the substation as LIBCS because the initial CIP-002-5.1 analysis determined there were only [redacted] lines, with connections to two other substations (weighted value of [redacted]) at the substation, when actually the substation had [redacted] lines, with connections to four other transmission assets (weighted value of [redacted]). Additionally, the substation had [redacted] ties to two different entities. Therefore, BES Cyber Systems should have been identified as MIBCS. The data for all other previously identified BES Cyber Systems was then compared and found to be consistent and did not yield any additional change to impact ratings. The newly categorized MIBCS did not have External Routable Connectivity (ERC). After reviewing all relevant information, WECC determined that the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2. Consequently, the entity did not apply the applicable CIP requirements to the MIBCS without ERC which it was required to have in place to comply with several other CIP Standards and Requirements. The root causes of the violation were less than adequate procedures, documents, and records to ensure proper evaluation of BES Assets. Specifically, the entity utilized an evaluation process that relied on outdated information and a manual review, which resulted in the entity overlooking critical information needed for identifying and categorizing the impact rating of a BES Cyber System. WECC determined that this issue began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on May 11, 2017, when the entity completed its Mitigation Plan.
Risk Assessment	This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2. The MIBCS in scope had no ERC. The number of CIP requirements applicable to MIBCS without ERC is limited. However, [redacted] had no additional controls to detect or prevent this violation from occurring or compensate for the potential harm. Nevertheless, no harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) updated its CIP-002 BES Cyber System list to include the reclassification of the BES Cyber System in scope, and obtained CIP senior management signature; 2) updated its BES Cyber Systems Identification process to incorporate the accurate data source for CIP-002 identification; 3) confirmed compliance or identified deficiencies with other applicable CIP Standards that require mitigation; and 4) mitigated all CIP compliance deficiencies resulting from the identification of the MIBCS without ERC, which included patch management, baseline configuration, and cyber vulnerability assessments.
Other Factors	WECC reviewed [redacted] internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. [redacted] [redacted]

	WECC considered [redacted] CIP-002-5.1 R1 compliance history in determining the disposition track. WECC considered [redacted] CIP-002-5.1 R1 compliance history to be an aggravating factor in the disposition determination.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017207	CIP-007-6	R1; P1.1	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on [redacted])	2/28/2017 (when [redacted] disabled the ports that were not needed)	Compliance Audit	1/8/2018	1/29/2018

Description of the Violation (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, or confirmed violation.)	During a Compliance Audit [redacted], WECC determined that [redacted] was in violation of CIP-007-6 R1 Part 1.1 Specifically, when [redacted] was preparing its baseline on a workstation classified as a BES Cyber Asset (BCA) associated with its Medium Impact BES Cyber System (MIBCS), it evaluated all ports, and those that were considered unneeded were slated for removal. During the audit, [redacted] provided the audit team a [redacted] that [redacted] on the BCA not reflected in the devices' baseline. Upon further review, [redacted] determined that the baseline was correct and that the unnecessary ports had been overlooked during the removal process. The BCA in scope is an engineering workstation in the primary Control Center's separate but associated data center, and is not actively used by [redacted] to monitor or control the supervisory control and data acquisition (SCADA) network. WECC concluded that [redacted] failed to ensure that only those logical network accessible ports that were determined to be needed on a BCA within the MIBCS were enabled. The root cause of the violation was due to an oversight by the employee responsible for disabling the ports who did not follow [redacted]'s documented procedure for disabling unneeded ports that were not part of the baseline configuration and the lack of an internal control to ensure employees followed the procedure. The violation duration was 242 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.
Risk Assessment	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, [redacted] failed to enable only logical network accessible ports that were determined to be needed. Such failure could result in a malicious actor gaining access to the BCA to cause harm to [redacted]'s SCADA system, which could affect [redacted]'s [redacted] and its [redacted]. However, [redacted] implemented access control at the Electronic Security Perimeter (ESP) to only allow approved traffic into the protected network. [redacted] also implemented [redacted] inside the ESP. Based on the controls in place, WECC determined the likelihood of the potential harm occurring was low.
Mitigation	To mitigate this violation, [redacted]: 1) disabled logical network ports determined to be unneeded on the BES Cyber Asset in scope; 2) updated documentation to require a [redacted] be performed each time a change is made to a baseline configuration and validate it against the baseline; 3) documented a process to periodically review baseline configurations against a report of open ports to ensure only necessary logical ports are open and that the baselines are accurate; 4) trained personnel on the updated documentation and processes; and 5) added CIP-007 as a regular agenda item for the monthly CIP Compliance meetings.
Other Factors	WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner. WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017016991	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on [redacted])	2/23/2017 (for Part 2.1 when [redacted] included patching sources in its patch management process) 9/21/2017 (for Parts 2.2 and 2.3 when [redacted] evaluated security patches and updated its mitigation plan)	Self-Report	8/2/2017	12/22/2017

Description of the Violation (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, or confirmed violation.)	On [redacted] submitted a Self-Report, stating that, [redacted] it was in violation of CIP-007-6 R2 Part 2.2. Specifically, [redacted] reported that, for three Cyber Assets classified as Bulk Electric System Cyber Assets (BCAs) it did not assess security patches after the initial review of security patches on July 1, 2016 was conducted, pursuant to CIP-007-6 R2 Part 2.2. The devices and software in scope support the primary and backup Control Centers containing a Medium Impact Bulk Electric System Cyber System (MIBCS). After reviewing all relevant information, WECC determined a scope increase from the original Self-Report. WECC identified three additional devices classified as Protected Cyber Assets (PCA), where [redacted] failed to maintain documentation that it had performed a patch evaluation at least once every 35 days, as required by Part 2.2. Additionally, [redacted] did not document a patch source as required by Part 2.1. for one Electronic Access or Monitoring System (EACMS) and seven Physical Access Control Systems (PACS). Lastly, WECC determined that [redacted] created a mitigation plan for security patches assessed and not applied; however, did not include specific implementation timeframes, as required by Part 2.3. The root cause of the violation was a less than adequate security patch management program for CIP compliance. Specifically, [redacted]'s lack of knowledge and understanding of CIP Standards resulted in the implementation of a less than adequate security patch management program. The violation duration was 237 days for Part 2.1 and 447 days for Parts 2.2 and 2.3. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.
Risk Assessment	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to evaluate security patches within 35 calendar days of the last evaluation; to document a patch source for applicable assets; to maintain documentation that it had performed patch evaluations once every 35 calendar days for its MIBCS and associated PCAs, EACMS and PACs, pursuant to CIP-007-5 R2 Parts 2.1, 2.2 and 2.3. Such failure could potentially result in a malicious actor using known attack methods to gain control of a BES Cyber System. If control was established, the malicious actor could cause reboots, freezes, or install malware in the systems. An attack on the devices in scope could cause disruption, restriction of visibility, or affect the operating capabilities of [redacted]'s systems which could lead to unintended consequences that could affect the BES. However, the likelihood of the risk occurring was significantly reduced by the preventative controls [redacted] had implemented. Specifically, [redacted] implemented protections at each Electronic Security Perimeter (ESP) to permit only allowed traffic into and out of the ESP as well as implementing Intrusion Detection System devices to each network to detect malicious code. Three of the devices in question were not connected to the public internet; had no browser access or email, and were protected by CIP controls in CIP-004, CIP-005, CIP-006 and CIP-007. Infractions related to the remaining eleven devices constituted documentation failures for the Standard, however the evaluations were being conducted. In addition, [redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that the likelihood of the potential harm occurring was low.
Mitigation	To mitigate this violation, [redacted]: 1) updated the patch tracking workbook to include and maintain a list of all applicable devices and software; 2) installed applicable patches where appropriate or mitigation plans with required implementation timeframes were developed and approved by the CIP senior manager; 3) reviewed other supporting documents to determine if additional updates were needed; 4) now maintains a list for all applicable devices under the purview of the system support group (i.e. EACMS, PACS, and BCA switches); and 5) added patch tracking to its bi-monthly CIP Compliance Meeting agenda. Regular discussions with an appropriate level of view will ensure maintenance and consistency across SCADA Support and Systems Support to continue to meet expectations over time.

Other Factors	WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner. WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017204	CIP-004-6	R4; P4.1, 4.2	Medium	Moderate	7/1/2016 (for Part 4.1 when the Standard became mandatory and enforceable on [redacted]) 10/1/2016 (for Part 4.2 when the Standard became mandatory and enforceable on [redacted])	12/8/2017 (when [redacted] updated documented authorization records for access granted, and verified CIP access against authorization records)	Compliance Audit	12/13/2017	1/29/2018

Description of the Violation (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, or confirmed violation.)

During a Compliance Audit [redacted] WECC determined that [redacted] was in violation of CIP-004-6 R4 Part 4.1 and Part 4.2.

Specifically, for CIP-004-6 R4 Part 4.1, WECC determined that [redacted] was not able to demonstrate that it implemented its access management program per its documented processes. [redacted] documented that it utilized an Access Request Form and a CIP-004 Access Management Program spreadsheet when authorizing electronic or unescorted physical access to its Medium Impact Bulk Electric System Cyber System (MIBCS) and their associated Cyber Assets or when authorizing access to designated storage locations. From July 1, 2016 through November 21, 2016, [redacted] granted electronic and/or unescorted physical access to its MIBCS and associated Cyber Assets to five employees without having completed [redacted]'s Access Request Form per [redacted]'s Access Management and Revocation Program and Procedure. Relating to CIP-004-6 R4 Part 4.2, [redacted] states in its Access Management and Revocation Program and Procedure that quarterly reviews are conducted by comparing Access Request Forms to its CIP Unescorted Physical Security Perimeter and Electronic Security Perimeter list. However, [redacted] did not utilize the Access Request Forms; therefore, [redacted] did not have dated documentation of the verification between the list of employees who have been authorized for access and the list of personnel who have access, at least one each calendar quarter.

WECC concluded that [redacted] used a process other than that which was documented and failed to update its documented process to authorize electronic access, unescorted physical access, and/or access to designated storage locations.

The root cause of the violation was management policy guidance or expectations were not well-defined, understood, or enforced. Specifically, [redacted] was new to CIP Standards and Requirements and its subject matter experts and compliance staff lacked understanding of required evidence and retention periods.

The violation duration was 525 days for Part 4.1 and 433 days for Part 4.2. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.

Risk Assessment

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to document dated authorization records and include a business need for access granting pursuant to CIP-004-6 R4 Part 4.1, and failed to verify once each calendar quarter that employees with CIP access had authorization records pursuant to CIP-004-6 R4 Part 4.2. Such failure could result in unauthorized employees having electronic access, unescorted physical access and/or access to designated storage locations containing BES Cyber System information. This access could intentionally or unintentionally lead to misuse of information or devices that support [redacted]'s compliance obligations; thereby potentially affecting the reliability of the BPS.

[redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that the potential likelihood of the harm occurring was low.

Mitigation

To mitigate this violation, [redacted]:

1) updated its Access Management and Revocation Program and Procedure to reflect current practices;
2) holds monthly meetings to discuss CIP compliance;
3) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual reviews, and revocations; and
4) provided training on the new Access Management and Revocation Program and Procedures.

Other Factors

WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.

WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017208	CIP-010-2	R1; P1.1, 1.2, 1.3, and 1.4	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on [redacted])	5/31/2017 (when baseline configurations were updated)	Compliance Audit	1/22/2018	2/26/2018

Description of the Violation (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, or confirmed violation.)

During a Compliance Audit [redacted], WECC determined that [redacted] was in violation of CIP-010-2 R1 Parts 1.1.4, 1.1.5, 1.2, 1.3 and 1.4.

Specifically, [redacted] failed to include [redacted] in its baseline configuration for [redacted] classified as Protected Cyber Assets; one Physical Access Control Systems (PACS) server; one supervisory control and data acquisition (SCADA) [redacted] classified as a Bulk Electric System (BES) Cyber Asset, one [redacted] and three [redacted] classified as Electronic Access Control or Monitoring Systems (EACMS), all associated with its Medium Impact Bulk Electric System (BES) Cyber System (MIBCS) pursuant to CIP-010-2 R1 Part 1.1.4.

WECC auditors also identified a PACS server that had a security patch update installed after the mandatory and enforceable date of July 1, 2016, that was not included on the device's baseline configuration pursuant to CIP-010-2 R1 Part 1.1.5. Lastly, for the PACS [redacted], [redacted] was not able to provide evidence that any of the required change management activities per CIP-010-2 R1 Parts 1.2, 1.3 and 1.4 had been performed when it installed [redacted] on the PACS [redacted] on January 30, 2017. The installation of this software would have caused a deviation from the device's baseline configuration.

WECC concluded that [redacted] failed to: 1) include logical network accessible ports in its baseline configuration for 10 devices; 2) include an installed security patch in the baseline configuration for one PACS [redacted]; and 3) provide evidence that it performed CIP-010-2 R1 Parts 1.1, 1.2, 1.3, and 1.4 for the installed security patch on the PACS [redacted].

The root cause of the violation was [redacted] not following its documented process. Specifically, [redacted] developed adequate documented processes to ensure compliance with CIP-010-2 R1; however, [redacted] did not have adequate internal controls to ensure those processes were followed.

The violation duration was 334 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.

Risk Assessment

This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to maintain baseline configurations to include logical network accessible ports and security patches applied to assets, and failed to perform required change management activities for BES Cyber Assets, EACMS, and PACS pursuant to CIP-010-2 R1 Parts 1.1, 1.2, 1.3, and 1.4. Such failure could result in a lack of protective measures for those ports due to not knowing which ports were accessible, which could lead to cyber security vulnerabilities in those network devices, thereby potentially affecting [redacted]'s [redacted] and its [redacted].

[redacted] did not implement adequate internal controls to ensure its documented processes for CIP-010-2 R1 were followed; to ensure potential incidents caused by poorly executed baseline configurations and change management processes would be minimized; and to detect baseline configuration errors and change management process exclusions. [redacted] is a small municipal power company. Based on this, WECC determined that the likelihood of the potential harm occurring was low.

Mitigation

To mitigate this violation, [redacted]:

1) updated the baseline configurations for the devices in scope;
2) updated its Change Control and Configuration Management Procedure to include the required use of a CIP-010 Change Request form for the documentation of all changes, including the verification that all CIP-005, CIP-007, and CIP-010 security controls are met and a step to update baseline configuration changes as required by CIP-010-2 R1 Part 1.3;
3) held a meeting to discuss the changes to the procedure and offer guidance to ensure the baselines are consistent, accurate, and updated quickly after a well-managed change to the CIP-010 R1 part 1.1 baseline component;
4) included baseline changes as a standing item for discussion and reinforcement at monthly CIP compliance meetings; and
5) will review all baselines, on an annual basis at the minimum, to ensure they are accurate and up-to-date.

Other Factors	WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner. WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017206	CIP-004-6	R5; P5.1	Medium	Moderate	8/24/2016 (when documented process were not followed)	12/8/2017 Mitigation Plan completion	Compliance Audit	12/8/2017	2/8/2018

Description of the Violation (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, or confirmed violation.)

During a Compliance Audit [redacted] WECC determined that [redacted] it was in violation of CIP-004-6 R5 Part 5.1.

Specifically, [redacted] was unable to demonstrate that it implemented its access management program per its documented processes. [redacted] documented that it utilized an Access Request Form and a CIP-004 Access Management Program spreadsheet when revoking electronic or unescorted physical access to its Medium Impact Bulk Electric System Cyber System (MIBCS) and their associated Cyber Assets. However, [redacted] was not able to provide evidence on the spreadsheet of one employee's unescorted physical access being revoked, nor did [redacted] provide any completed Access Request Forms as stated in its process document.

Additionally, [redacted] was unable to provide evidence demonstrating that the process to remove one retiring employee's unescorted physical access was initiated upon a termination action and the removals completed within 24 hours of the termination action. WECC reviewed an email dated August 23, 2016, which [redacted] submitted as evidence demonstrating the removal of an employee's ability for unescorted physical access upon a termination action. The email stated that an employee no longer worked for the City and should no longer have access to the primary and backup Control Centers; however, the email contained no confirmation that the employee's unescorted physical access had been removed within 24 hours of the termination action, nor was [redacted] able to provide system logs to confirm access revocation had occurred within 24 hours of the termination action.

After reviewing all relevant information, WECC determined a decrease in scope from the original audit finding. Subsequent to the audit, [redacted] was able to provide WECC evidence that demonstrated compliance of revocation of unescorted physical access for the one employee in scope. However, WECC determined that [redacted] did fail to follow its documented processes for initiating removal of an employee's ability for CIP access upon a termination action.

The root cause of the violation was management policy guidance or expectations were not well defined, understood, or enforced. Specifically, [redacted] staff lacked the understanding of required evidence to demonstrate compliance and the retention periods for said evidence.

The violation duration was 471 days. [redacted] did not have detective controls in place that could have helped identify the issues sooner and to lessen the violation duration. WECC believes had it not been for [redacted]'s Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied an aggravating factor and escalated the disposition treatment to an expedited settlement.

Risk Assessment

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, [redacted] failed to provide evidence to demonstrate the removal of the ability for access or the actual unescorted physical access within 24 hours after a termination action. Such failure could result in unauthorized physical access to BES Cyber Systems with the intent to cause damage or outages; thereby potentially affecting the reliability of the BPS.

[redacted] is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determined that likelihood of the potential harm occurring was low.

Mitigation

To mitigate this violation, [redacted]:

1) updated its Access Management and Revocation Program and Procedure to reflect current practices and detailed tracking of CIP access management;
2) holds monthly meetings to discuss CIP compliance;
3) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual reviews, and revocations; and
4) provided training on the new Access Management and Revocation Program and Procedures.

Other Factors

WECC reviewed [redacted]'s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although [redacted] has a documented ICP, WECC determined that [redacted] did not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.

WECC considered [redacted]'s compliance history and determined there were no relevant instances of noncompliance.