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	NPCC2018020059	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
2	NPCC2018020060	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
3	NPCC2018020061	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
4	NPCC2018020063	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
5	NPCC2018020064	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
6	NPCC2018020062	Yes		Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
7	WECC2017018752	Yes		Yes	Yes				Yes					Category 1: 3 years; Category 2 – 12: 2 year
8	WECC2018019340	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
9	WECC2017018489	Yes		Yes	Yes				Yes				Yes	Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2017018732	Yes		Yes	Yes				Yes					
11	WECC2017017229	Yes		Yes	Yes	Yes	Yes		Yes					
12	WECC2018020044	Yes		Yes	Yes				Yes					
13	WECC2018020045	Yes		Yes	Yes	Yes	Yes		Yes					
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														

Filing Date: June 27, 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
NPCC2018020059	CIP-002-5.1a	R1. (1.1., 1.2., 1.3.).	High	Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted] was in violation of CIP-002-5.1a R1. (1.1., 1.2., 1.3.). [redacted]

This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low impact, and that is why they failed to update the documentation.

The root cause of this violation was lack of accountability and management oversight.

Risk Assessment

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

Mitigation

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

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
NPCC2018020059	CIP-002-5.1a	R1. (1.1., 1.2., 1.3.).	High	Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors	NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to update its documentation to identify the BES Cyber Systems as required by the Standard.								

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
NPCC2018020060	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined stating that [redacted] (the entity) as a [redacted] was in violation of CIP-002-5.1a R2. (2.1., 2.2.). [redacted]

This violation started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its CIP Senior Manager or delegate approve the identifications. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets and had its CIP Senior Manager approve the identifications.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low, and that is why they failed to update documentation.

The root cause of this violation was lack of accountability and management oversight.

Risk Assessment

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify, review and have its CIP Senior Manager approve BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

Mitigation

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

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
NPCC2018020060	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors	NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to have a CIP Senior Manager approve the impact ratings as required by the Standard.								

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
NPCC2018020061	CIP-003-6	R3.	Medium	VSL - Severe	July 1, 2016	December 1, 2016	Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined that [redacted] as a [redacted] was in violation of CIP-003-6 R3. [redacted] This violation started on July 1, 2016 when the entity failed to identify a CIP Senior Manager by name. The violation ended on December 1, 2016 when the entity designated a CIP Senior Manager. Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. The root cause of this violation was lack of accountability and management oversight.
Risk Assessment	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections. [redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted] [redacted] Additionally, the facility has a 24 hour start-up time and only runs when needed. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this violation, the entity: 1) Designated a CIP Senior Manager To prevent recurrence, the entity: 2) Created automated tasks to maintain documentation for CIP Senior Manager designations.
Other Factors	NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity'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
NPCC2018020063	CIP-002-5.1a	R1. (1.1., 1.2., 1.3.).	High	VSL -Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined that [redacted] the entity) as a [redacted] was in violation of CIP-002-5.1a R1. (1.1., 1.2., 1.3.). [redacted]

This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low impact, and that is why they failed to update the documentation.

The root cause of this violation was lack of accountability and management oversight.

Risk Assessment

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

Mitigation

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

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
NPCC2018020063	CIP-002-5.1a	R1. (1.1., 1.2., 1.3.).	High	VSL -Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to update its documentation to identify the BES Cyber Systems as required by the Standard.						

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
NPCC2018020064	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted], was in violation of CIP-002-5.1a R2. (2.1., 2.2.). [redacted]

This violation started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its CIP Senior Manager or delegate approve the identifications. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets and had its CIP Senior Manager approve the identifications.

Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low, and that is why they failed to update documentation.

The root cause of this violation was lack of accountability and management oversight.

Risk Assessment

The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify, review and have its CIP Senior Manager approve BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.

The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.

[redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted]

[redacted]

Additionally, the facility has a 24 hour start-up time and only runs when needed.

No harm is known to have occurred as a result of this noncompliance.

Mitigation

To mitigate this violation, the entity:

1) Updated its CIP-002 procedure to Version 5
2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems.

To prevent recurrence, the entity:

3) Implemented software to create and track tasks. The system will send multiple automatic email reminders to the responsible person until the task is completed. The system will also send escalation emails to overseeing persons if the task has not been completed within a specified amount of time. Tasks will repeat upon closure or with a specified frequency depending on how they are set up.

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
NPCC2018020064	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors	NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to have a CIP Senior Manager approve the impact ratings as required by the Standard.								

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
NPCC2018020062	CIP-003-6	R3.	Medium	VSL - Severe	July 1, 2016	December 1, 2016	Off-site Audit	12/14/2018	12/18/2018

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 conducted from [redacted], NPCC determined that [redacted] (the entity) as a [redacted] it was in violation of CIP-003-6 R3. [redacted] This violation started on July 1, 2016 when the entity failed to identify a CIP Senior Manager by name. The violation ended on December 1, 2016 when the entity designated a CIP Senior Manager. Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. The root cause of this violation was lack of accountability and management oversight.
Risk Assessment	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections. [redacted] All visitors to the site (except visitors who will only be in the office area) are required to sign into the control room's visitor's log. Stating their name, date, reason for visit and the name of their entity contact. [redacted] Unauthorized personal are not allowed in these areas without a company escort or expressed permission from the plant manager. [redacted] [redacted] Additionally, the facility has a 24 hour start-up time and only runs when needed. No harm is known to have occurred as a result of this noncompliance.
Mitigation	To mitigate this violation, the entity: 1) Designated a CIP Senior Manager To prevent recurrence, the entity: 2) Created automated tasks to maintain documentation for CIP Senior Manager designations.
Other Factors	NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity'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
WECC2017018752	CIP-007-6	R5; P5.5	Medium	Severe	11/2/2016 (when password length and complexity was not enforced)	12/14/2016 (when password length and complexity were enforced)	Self-Report	11/6/2017	9/20/2018

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.)	On December 5, 2017, the entity submitted a Self-Report stating that, as a as a [redacted] it was in violation with CIP-007-6 R5. Specifically, the entity reported that on November 2, 2016, while changing passwords for non-CIP devices, an employee from its [redacted]) team also changed the passwords of two BES Cyber Assets (BCAs) using the same password requirements of the non-CIP devices which was [redacted]. The two BES Cyber Assets (BCAs) were associated with a Medium Impact BES Cyber System (MIBCS) at the primary and backup Control Center. The entity's [redacted] policy clearly documents the password complexity parameter requirements of CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2 for CIP devices. The employee was authorized to change passwords for both CIP and non-CIP devices. The entity discovered this noncompliance on December 9, 2016 during its quarterly access review. After reviewing all relevant information, WECC determined the entity failed to implement its documented process for password-only authentication for interactive user access when it did not enforce password parameters for length and complexity, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2. The root cause of the violation was incorrect performance due to lack of process controls around password changes. Specifically, an employee tasked with changing the passwords of non-CIP devices also changed the passwords on two BCAs while performing routine tasks on the non-CIP devices. This violation began on November 2, 2016, when password length and complexity was not enforced on two BCAs, and ended on December 14, 2016, when the entity enforced the password length and complexity on the two BCAs, for a total of 43 days of noncompliance.
Risk Assessment	WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to implement its documented process for password-only authentication for interactive user access when it did not enforce password parameters for length and complexity, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2. The entity implemented good compensating controls. [redacted] No harm is known to have occurred.
Mitigation	To remediate and mitigate this violation, the entity: a. changed the password length and complexity on the BCAs in scope; b. held a "Fact Finding" meeting with members of the [redacted] team to discuss the CIP asset password policy and employee responsibilities related to the importance of following document processes; and c. reconfigured the BCAs in scope to no longer be CIP assets resulting in the [redacted] team no longer having responsibility for CIP assets.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity has implemented a comprehensive and well organized ICP. Within its ICP is a risk assessment process in which the entity analyzes risk through collaboration between several areas of the company. The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.

	WECC considered the entity's CIP-007-6 R5 compliance history in determining the disposition track. WECC considered the entity's CIP-007-6 R5 compliance history to be an aggravating factor in determining the disposition track.

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
WECC2018019340	CIP-007-6	R2; P2	Medium	Severe	9/7/2017 (when cyber security patches were not tracked)	2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates)	Self-Certification	8/14/2018	9/24/2018

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.)

On March 1, 2018, the entity submitted a Self-Certification stating that as a [redacted], it was in violation with CIP-007-6 R2.

Specifically, the entity reported that during its Self-Certification review on January 16, 2018, the CIP Lead discovered that commercial software had not been evaluated for security patch applicability that was installed on two Electronic Access Control and Monitoring Systems (EACMS) Cyber Assets associated with a MIBCS at its primary and backup Control Centers. [redacted]. The entity tracked software applicable to its [redacted]" spreadsheet. The [redacted] software had been removed from that list in error. The spreadsheet listed the version of the [redacted] software residing on a single Physical Access Control System (PACS) Cyber Asset as the version in question. The version of [redacted] software residing on the EACMS Cyber Assets was listed on the spreadsheet incorrectly. Earlier in the year, the responsible engineer removed the PACS Cyber Asset from its association to a BES Cyber System. As that was the only Cyber Asset listed on the spreadsheet as containing the [redacted] software, the Cybersecurity Supervisor assumed that all instances of said software had been removed from all MIBCS and associated Cyber Assets. He therefore annotated the entry on the spreadsheet as no longer requiring assessment, when in fact a version of the [redacted] software was still residing on the two EACMS Cyber Assets.

After reviewing all relevant information, WECC determined the entity failed to appropriately implement its patch management process to track, evaluate, and install cyber security patches for applicable Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3, respectively.

The root cause of the violation was a less than adequate security patch management tracking process. Specifically, the task of when and how to remove a source from the security patch tracking list was not covered in the documented process.

This violation began on September 7, 2017, when cyber security patches for the two EACMS should have been tracked, and ended on February 20, 2018, when the entity tracked, evaluated, and applied applicable software updates, for a total of 167 days of noncompliance.

Risk Assessment

WECC determined that this 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 appropriately implement its patch management process to track, evaluate, and install cyber security patches for applicable Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists; at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3, respectively.

However, the entity implemented good compensating controls. [redacted] No harm is known to have occurred.

Mitigation

To remediate and mitigate this violation, the entity:

a. evaluated the commercial software updates released since August 2, 2017;
b. applied applicable security patches to the EACMS Cyber Assets in scope;
c. in conjunction with the commissioning of the new Energy Management System (EMS), update its Security Patch Management Program, to include vendor supported monitored of security patches for the new EMS; and
d. provided training to stakeholders on the updates to the Security Patch Management Program.

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
WECC2018019340	CIP-007-6	R2; P2	Medium	Severe	9/7/2017 (when cyber security patches were not tracked)	2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates)	Self-Certification	8/14/2018	9/24/2018

Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity has implemented a comprehensive and well organized ICP. Within its ICP is a risk assessment process in which the entity analyzes risk through collaboration between several areas of the company. The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance. WECC considered the entity's CIP-007-6 R2 compliance history in determining the disposition track. WECC considered the entity's CIP-007-6 R2 compliance history to be an aggravating factor in determining the disposition track.

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
WECC2017018489	CIP-003-2	R4	Medium	Severe	9/22/2010	7/12/2017	Self-Report	11/8/2017	7/13/2018

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.)	On October 18, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-003-2 R4. Specifically, the entity reported that on September 22, 2010, an employee from the [redacted] group had inadvertently uploaded Critical Cyber Asset (CCA) information to the [redacted] file share. On July 11, 2017 the [redacted] group discovered the CCA information and notified the [redacted] group. [redacted] examined the information that was stored on the [redacted] file share and found that it was CCA Information as defined by the entity's [redacted] Program and should have been protected according to the program. With further examination of the security permissions associated with the [redacted] file share, the [redacted] group noted 14 unauthorized individuals with access to the CCA information. The CCA information on the [redacted] file share included all [redacted] On July 12, 2017, the [redacted] group removed the CCA information from the [redacted] file share. After reviewing all relevant information, WECC determined the entity failed to implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-2 R4. The root cause of the violation was an individual who did not follow the procedures the entity had in place. Specifically, the individual who placed the CCA information on the [redacted] file share did not follow the expectations outlined in the entity's Information Protection Program.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-2 R4. The entity had implemented weak controls to prevent and/or detect the noncompliance. However, the entity had compensating controls in place that lessened the risk. Access to the CCA information by someone with malicious intent would not have provided any direct physical or electronic access to the High Impact BES Cyber Systems (HIBCS) or Medium Impact BES Cyber Systems (MIBCS); the access simply provided information that might be used to exploit a vulnerability in the entity's defenses if a malicious actor was able to penetrate the perimeter defenses. The entity had also implemented a defense-in-depth approach to cyber security. [redacted] No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) removed the CCA information from the [redacted] file share; 2) created a secure [redacted] file share that is designated as a BES Cyber System Information (BCSI) repository with all the appropriate controls; and 3) conducted BCSI Protection Program training with appropriate individuals.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. However, it is worth noting that the violation duration for CIP-003-2 R4 is significant and should have been found much sooner, had the entity had better internal controls in place; especially considering the implementation of later versions of the Standard and Requirement. WECC considered the entity's CIP-003 R4 compliance history in determining the penalty. WECC considered the entity's CIP-003 R4 compliance history to be an aggravating factor in the penalty 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
WECC2017018732	CIP-007-6	R5	Medium	Severe	7/1/2016	2/13/2018	Self-Report	8/15/2018	TBD

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 4, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-007-6 R5. Specifically, the entity reported that on July 17, 2017, it discovered multiple devices that did not have methods to enforce authentication of interactive user access. Upon further review conducted on July 26, 2017, the entity verified that three [redacted] Cyber Assets, categorized as Protected Cyber Assets (PCAs) associated with the Medium Impact BES Cyber Systems (MIBCS) without External Routable Connectivity (ERC) at three separate substations did not have passwords. The PCAs contained software and applications written in-house by the entity and an administrator account where the password functionality had not been enabled. The PCAs had been designated to monitor and control the health of three [redacted] at two of the substations, and to monitor and control a [redacted] and [redacted] at a third substation. When CIP-007 Version 5 went into effect, these Cyber Assets were not updated to enforce authentication of interactive user access because of potential operational and safety impacts, as well as a lack of clarity over the interpretation of the Requirement. If the PCA lost communication to the [redacted], designated as BES Cyber Assets (BCAs), for any reason, [redacted] This delay would have caused [redacted] into the [redacted] which the entity believes would have introduced risk to the reliability of the BES. After reviewing all relevant information, WECC determined the entity failed to have a method(s) to enforce authentication of interactive user access, where technically feasible; change known default passwords, per Cyber Asset capability; and for password-only authentication for interactive user access, either technically or procedurally enforce password parameters, as required by CIP-007-6 R5 Parts 5.1, 5.4, and 5.5 Sub-Parts 5.5.1 and 5.5.2, respectively for three PCAs. The root cause of the violation was an insufficient number of trained or experienced employees assigned to a task. Specifically, in its transition to CIP Version 5, the entity did not ensure that the persons responsible for identifying and implementing security controls for PCAs had adequate training and/or experience to appropriately protect them.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to have a method(s) to enforce authentication of interactive user access, where technically feasible; change known default passwords, per Cyber Asset capability; and for password only authentication for interactive user access, either technically or procedurally enforce password parameters, as required by CIP-007-6 R5 Parts 5.1, 5.4, and 5.5 Sub-Parts 5.5.1 and 5.5.2, respectively. The entity had implemented weak controls to prevent and/or detect this noncompliance. However, the entity had compensating controls in place that lessened the risk. [redacted] No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) adjusted the operability of the applications on the PCAs to allow for password functionality. This step will take programmatic and/or configuration changes to ensure that the devices and associated applications operate as expected with the enablement of the password functionality. These changes will need to be tested and implemented and are complicated by the fact that the devices are located [redacted]; 2) enabled the password functionality on the three PCAs to implement authentication of user access; 3) changed the default password on the three PCAs; and 4) had [redacted] meet with the group responsible for the PCAs to review and discuss the [redacted] procedures. This discussion included specific training related to actions required for default and generic account passwords.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC considered the entity's CIP-007 R5 compliance history in determining the penalty. WECC considered the entity's CIP-007 R5 compliance history to be an aggravating factor in the penalty 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
WECC2017017229	CIP-011-2	R1	Medium	Severe	8/12/2016	8/31/2016	Self-Report	3/1/2017	1/31/2018

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.)	On January 30, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-011-2 R1. Specifically, the entity's [redacted] group utilized the [redacted] application as a patching tool for the Microsoft devices in its High Impact BES Cyber Systems (HIBCS) and associated Electronic Access Control and Monitoring System devices (EACMS) within the [redacted]. To ensure the protection of the HIBCS and [redacted] and associated critical devices in the secure environment, the [redacted] group had utilized a [redacted] approach. The first server resided [redacted] and contained all the pertinent information about Microsoft devices that required patches and updates, which included the [redacted] of the applicable BCAs and PCAs within the HIBCS ESP. The second server resided [redacted] This [redacted] was fully controlled by [redacted] personnel and also contained pertinent information about Microsoft devices that required patches and updates, which included [redacted] of the applicable EACMS within the [redacted]. In accordance with the entity's [redacted] Program, the entity had identified and classified the information on the first and second server as BCSI. The third server resided [redacted], on the entity's [redacted] and [redacted] for the applicable BCAs, PCAs, and EACMS. This server did not contain any IP addresses or host names that would be considered BCSI, but rather the server [redacted]. The [redacted] setup was utilized to ensure that the HIBCS and EACMS were isolated from direct internet connectivity. [redacted] In the spring of 2016, the entity's [redacted] group began experiencing technical issues with the [redacted] application at which time they reinstalled the [redacted] application and reconfigured all [redacted]. The reconfiguration was completed on August 12, 2016. However, on August 26, 2016, the entity's [redacted] group notified the [redacted] department that the [redacted] application setup process inadvertently [redacted] of all its Windows-based HIBCS BCAs and associated Windows-based PCAs, as well as all the EACMS devices, onto a server in its [redacted]. Once the issue was discovered, the entity's [redacted] group took immediate steps to correct the issue: 1) they deleted the [redacted] server's [redacted] database that contained all the [redacted]; 2) on August 31, 2016, they deleted all of the backups of the [redacted] server's [redacted] database that had been created since the reinstall from August 12, 2016 to August 26, 2016. After reviewing all relevant information, WECC determined the entity failed to protect and securely handle its BCSI while in storage as required by CIP-011-2 R1 Part 1.2. The root cause of the violation was a less than adequate review of work. Specifically, due to a configuration error in the [redacted] application, BCSI was replicated outside the secured CIP environment, and the entity had no peer review process in place to ensure the application was setup correctly.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to protect and securely handle its BCSI while in storage as required by CIP-011-2 R1 Part 1.2. The entity had implemented weak controls to prevent this noncompliance. However, the entity had compensating controls in place that lessened the risk. The limited exposure of the BCSI to internal employees was restricted to those who have elevated privileges within the entity's environment and all have a valid business need for access to the [redacted] server. The BSCI that was exposed did not contain usernames or passwords. Without this information, it would be difficult for a person with malicious intent to access any of the devices within the HIBCS or [redacted] Lastly, the entity has a [redacted]. No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) deleted its [redacted] server database files and associated backups; 2) implemented an automated system in order to avoid manual configuration errors and the need for manual reviews of work; and 3) implemented a third-party patching solution that prevents BSCI from being replicated outside of the ESP or [redacted] to avoid future issues with manual patching.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC considered the entity'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
WECC2018020044	CIP-011-2	R1	Medium	Severe	7/1/2016	1/25/2017	Self-Report	12/19/2017	1/31/2018

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.)	On January 30, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-011-2 R1. Specifically, the entity reported that it utilized a baselining tool to scan devices within its Physical Access Control System (PACS) environment to gather information related to baseline configurations, device ports, services, accounts, and other information used to meet CIP compliance. The scan engine, which was part of the baselining tool, was located on [redacted] and was used to run scans against PACS assets [redacted]. The scan engine reports the results back to the baselining tool management console where they were kept [redacted]. The baselining tool management console controls the scan engine, telling it where to scan, when to scan, what to scan for, etc. The baselining tool database resides [redacted] On September 28, 2016, during a review of its systems, the entity discovered that both the baselining tool database and management console were not designated as BSCI repositories; therefore, they did not have the protective CIP controls that would normally be applied to BCSI. The missing controls included [redacted] as required by CIP-004-6 R4 Part 4.1.3, and [redacted] After reviewing all relevant information, WECC determined the entity failed to appropriately identify BCSI associated with its PACS, as required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS data in the baselining tool as BCSI resulted in it not being identified as a BCSI repository, which in turn caused the entity to not provide the appropriate authorized electronic and physical access controls as required by CIP-004-6 R4 Part 4.1.3. The root cause of the violation was the entity's oversight of a critical device which led to the misidentification of the information contained within the device that should have been classified as restricted and therefore protected as BCSI.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to appropriately identify BCSI associated with its PACS, as required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS data in the baselining tool as BCSI resulted in it not being identified as a BCSI repository, which in turn caused the entity to not provide the appropriate authorized electronic and physical access controls as required by CIP-004-6 R4 Part 4.1.3. The entity had implemented weak controls to prevent and/or detect this noncompliance. However, the entity had compensating controls in place that lessened the risk. The limited exposure of the BCSI to internal employees was restricted to those who had elevated privileges within the entity's environment and all had a valid business need for access. In addition, all [redacted] was logged and, as needed, [redacted]. Lastly, the entity's [redacted] No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) identified the PACS data as BCSI; 2) added the baselining tool database and management console servers to a [redacted] and designated them as BCSI repositories; 3) deleted all baselining tool backups in the [redacted] and rescheduled future backups to the [redacted]; 4) updated its process to include accurate information and expectations regarding this Standard and Requirement; 5) updated its procedure to include a specific email to be utilized for PACS-related questions; and 6) added access controls: i) authorization process to access [redacted]; and ii) established shared account password management; a) all account passwords were reset with system-generated strong passwords; b) account passwords [redacted]; and c) account passwords [redacted].
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC considered the entity'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
WECC2018020045	CIP-011-2	R1	Medium	Severe	1/12/2017	1/12/2017	Self-Report	12/19/2017	1/31/2018

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.)	On May 1, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-011-2 R1. Specifically, the entity reported that on January 12, 2017, its [redacted] group was notified of an event related to an employee potentially sending [redacted] BCSI to an external company earlier that day. The employee stated that errors began occurring with a [redacted] server and since an [redacted] "go live" was a few days away, the employee contacted the [redacted] Customer Support group for resolution. [redacted] provided the software that integrates the [redacted] to the [redacted]. The [redacted] Customer Support requested the employee send the entity's [redacted] configuration database to them so that they could troubleshoot the issues. The employee did not think there was an issue with sending the entity's [redacted] configuration database to [redacted] Customer Support group because: (1) the entity had a signed Mutual Nondisclosure & Confidentiality Agreement (MNDA) with [redacted]; (2) the information [redacted] was requesting was typical configuration database information for a vendor to have; and (3) the employee believed that the configuration database file would not be human readable. The employee was aware of the entity's [redacted] Program requirement to encrypt BCSI sent externally but at the time she did not know the information within the configuration database file was BCSI. Therefore, the employee sent the [redacted] configuration database file, [redacted] by email. After sending the email, the employee opened the configuration database file and realized it included [redacted] The [redacted] servers were MIBCS BCAs and resided in an [redacted], between the HIBCS [redacted] and the MIBCS [redacted]. The purpose of the [redacted] servers was to send and receive [redacted] data for use in the entity's HIBCS. After reviewing all relevant information, WECC determined the entity failed to securely handle its BCSI during transit, as required by CIP-011-2 R1 Part 1.2. The root cause of the violation was an omission of steps based on assumption. Specifically, the employee that sent the data to an external vendor assumed that it was not BCSI and did not confirm those assumptions prior to sending BCSI [redacted] by email.
Risk Assessment	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to securely handle its BCSI during transit, as required by CIP-011-2 R1 Part 1.2. The entity had implemented weak controls to prevent this noncompliance. However, the entity had compensating controls in place that lessoned the risk. The limited exposure of the BCSI to an external source was restricted to a vendor where an NDA already existed and was in effect. The BSCI that was exposed did not contain usernames or passwords. Without this information, it would be difficult for a person with malicious intent to access any of the devices within the HIBCS or MIBCS. No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity: 1) requested and confirmed [redacted] destroyed all copies of the BCSI that was emailed; and 2) provided additional CIP Access Training, which included training on its [redacted] Program, to the employee who sent the [redacted] email.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.