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	TRE2016016184	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 year

Filing Date: September 26, 2019

[redacted] NOC-2646 No penalty

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
TRE2016016184	CIP-002-5.1	R1	High	Lower	7/1/2016 (when the Standard became mandatory and enforceable)	Present	Self-Certification	11/7/2019 (approved completion date)	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 [redacted], the Entity submitted a Self-Certification stating that, as a [redacted], it was in noncompliance with CIP-002-5.1 R1. Specifically, the Entity did not have or implement a process that considers [redacted] for the purposes of CIP-002-5.1 R1, Parts 1.1 through 1.3. As a result, the Entity did not identify each asset that contains a BES Cyber System. This issue began when CIP-002-5.1 became enforceable and continued after CIP-002-5.1a R1 became enforceable. The root cause of this issue is that the Entity did not have any documented process for compliance with CIP-002-5.1 during the period leading up to CIP-002-5.1 becoming enforceable. As a result, the Entity did not document or implement processes necessary for compliance with CIP-002-5.1. This noncompliance started on July 1, 2016, when CIP-002-5.1 R1 became enforceable and is currently ongoing.
Risk Assessment	This issue posed a moderate risk and did not pose a serious or substantial risk to the bulk power system based on the following factors. The failure to properly identify and classify a BES Cyber System increases the potential that the BES Cyber System will not receive the appropriate cyber security protections. The duration of this issue was approximately three years, lasting from July 1, 2016, when CIP-002-5.1 became enforceable, until the present. In addition, during the noncompliance, the Entity's [redacted] In addition, the Entity's initial review of its assets indicates that the Entity [redacted] BES Cyber Systems.
Mitigation	To mitigate the noncompliance, the Entity: 1) created a draft process for compliance with CIP-002-5.1a, which includes a preliminary draft of the identifications required by CIP-002-5.1a R1; 2) approved a documented internal compliance program, which includes a process for identifying applicable current and new Reliability Standards; 3) established a compliance committee, as described in the documented internal compliance program, which determines upcoming deadlines at regular meetings and implements the Entity's process for identifying applicable Reliability Standards; and 4) conducted training regarding the Entity's process for compliance with CIP-002-5.1a and regarding the Entity's overall compliance program. Furthermore, the Entity submitted a Mitigation Plan to address the following actions that will be completed by November 7, 2019: 1) finalize and have CIP Senior Manager approve the draft identifications required by CIP-002-5.1a R1. The Entity requires [redacted] and intends to complete this change before finalizing its process for compliance with CIP-002-5.1a R1.
Other Factors	[redacted] Texas RE considered the Entity's compliance history and determined there were no relevant instances of noncompliance.

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	MRO2017018152	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years
2	MRO2017018150	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 – 12: 2 years

Filing Date: August 29, 2019

[redacted] ("the Entity") NOC-2645 $0

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
MRO2017018152	CIP-007-6	R5.7	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable)	10/31/2018 (when all applicable Cyber Assets were configured to either lockout or send a real-time alert)	Compliance Audit	2/25/2019	2/25/2019

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], MRO determined that the Entity, as a [redacted] was in violation of CIP-007-6 R5. Sampling conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber Assets that were not configured to either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, as required by P5.7. The cause of the noncompliance was the Entity's failure to understand the full scope of the Standard and Requirement. The Entity believed that it was not required to file a Technical Feasibility Exception (TFE) if the device could not meet the requirements. Additionally, the Entity only considered whether a device had the capability to limit the number of unsuccessful authentication attempts, and failed to consider a device's event forwarding capability in conjunction with a collection system(s) that can generate an alert as a method for complying with P5.7.
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 (BPS). Two of the devices were granted a TFE that resolved the noncompliance. One of the devices had a low inherent risk to the BPS as it was a terminal server that transferred redundant information to map boards. The majority of remaining devices were receiving some level of protection at the time of the Compliance Audit. Prior to the audit, event forwarding had been turned on for these devices, which were configured to alert through an hourly report (MRO does not consider an alert from an hourly report to be compliant with P5.7). Finally, the Entity's [redacted] No harm is known to have occurred.
Mitigation	To mitigate this violation, the Entity: 1) submitted a TFE for two devices; 2) conducted an extent of condition review; 3) configured all applicable devices to either lockout or send a real-time alert; 4) augmented the account implementation form to add additional steps and permit the elevation of concerns for peer or supervisory review; and 5) validated updated process and provided training to SMEs through a table top exercise of actual assessment of applicable Cyber Asset(s).
Other Factors	MRO considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applicable devices should be self-detected through internal controls. However, MRO determined that even though the noncompliance should not be eligible for Compliance Exception treatment, the noncompliance does not warrant a financial penalty given the minimal impact of the noncompliance upon the BPS. MRO considered the Entity's CIP-007-6 R5 compliance history in determining the penalty. MRO determined that the Entity's compliance history should not serve as a basis for aggravating the penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not caused by a failure to mitigate the prior noncompliance.

[redacted] ("the Entity") NOC-2645 $0

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
MRO2017018150	CIP-010-2	R1.1.2	Medium	Lower	7/1/2016 (when the Standard became mandatory and enforceable)	5/11/2018 (updated the existing baselines to include all intentionally installed software)	Compliance Audit	2/25/2019	2/25/2019

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], MRO determined that the Entity, [redacted], was in violation of CIP-010-2 R1. Sampling conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber Assets that did not have baselines that included all installed commercially available software as required by P1.1. The Entity did not include the [redacted] software on the documented baseline for two devices and the Entity did not sufficiently identify the [redacted] software for numerous devices. The Entity would typically document its baselines in either its baseline tool or its patch management system (an alternate tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. The [redacted] software was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber Asset. The Entity did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible discrepancies. The cause of the noncompliance was the Entity's deficient process for developing baselines and detecting errors or omissions.
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 (BPS). For all affected Cyber Assets, with the exception of two, the noncompliance was limited to not including sufficient detail regarding the software version as opposed to an omission. Further, the Entity had a software change process and change form specifically for the [redacted] software, reducing the risk of an inadvertent or unapproved change. The [redacted] software was also well managed by the Entity's SMEs, reducing the risk of an unexpected change to the [redacted] software. Finally, the Entity's [redacted]. No harm is known to have occurred.
Mitigation	To mitigate this violation, the Entity: 1) conducted an extent of condition analysis; 2) corrected the baselines for the impacted Cyber Assets; 3) improved the process to identify any commercially available software; and 4) validated the new process of identifying any commercially available or intentionally installed software.
Other Factors	MRO considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applicable devices should be self-detected through internal controls. However, MRO determined that even though the noncompliance should not be eligible for Compliance Exception treatment, the noncompliance does not warrant a financial penalty given the minimal impact of the noncompliance upon the BPS. MRO considered the Entity's compliance history and determined there were no relevant instances of noncompliance.

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	NPCC2018020347	Yes		Yes	Yes					Yes				Categories 3 – 4: 2 years Categories 1, 9: 3 years
2	NPCC2018020348	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
3	NPCC2018020350	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
4	NPCC2018020346	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
5	NPCC2018020351	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
6	WECC2018020039			Yes	Yes				Yes					Category 2 – 12: 2 year
7	WECC2018020282			Yes	Yes									Category 2 – 12: 2 year
8	WECC2016015862			Yes	Yes							Yes	Yes	Category 2 – 12: 2 year
9	WECC2017018174	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2017017885	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
11	WECC2018019006			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
12	WECC2017016941	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
13	WECC2017016928	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
14	WECC2017016939	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
15	WECC2017016938			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
16	WECC2017016940	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
17	WECC2017016926	Yes		Yes	Yes				Yes	Yes	Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 year
18	WECC2017016929			Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														

[redacted] NOC-2636 $10,000

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
NPCC2018020347	CIP-002-5.1a	R1.1, R1.2, R1.3	High	Lower	3/29/2017	9/4/2018	Self-Report	9/4/2018	12/12/2018

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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-002-5.1a R1. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program. This violation started on March 29, 2017 when the entity failed to implement a process to identify its BES Cyber Systems. The violation ended on September 4, 2018 when the entity developed a process for identifying and rating its BES Cyber Systems. Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted].
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 the impact level of its assets, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a Process Information (PI) system that is used for real-time performance monitoring and diagnostics. This system sends information to [redacted]; if this connection were interrupted, the entity would provide data to [redacted] via phone. The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted].
Mitigation	To mitigate this violation, the entity: 1. contracted third-party company to create compliance program; and 2. developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1. To prevent recurrence, the entity: 1. implemented automated system/tasks to ensure NERC activities are tracked and completed.
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 and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.

[redacted] NOC-2636 $10,000

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
NPCC2018020348	CIP-002-5.1a	R2.1, R2.2	Lower	High	3/29/2017	9/4/2018	Self-Report	9/4/2018	12/12/2018

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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered on June of 2017 it was in noncompliance with CIP-002-5.1a R2. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program. This violation started on March 29, 2017 when the entity failed to implement a process to identify its BES Cyber Systems, and therefore did not review or have CIP Senior Manager Approval of the identified impact levels. The violation ended on September 4, 2018 when the entity developed a process for identifying and rating its BES Cyber Systems, designated a CIP Senior Manager and reviewed and approved its identified impact level. Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted].
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 the impact level of its assets, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone. The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted].
Mitigation	To mitigate this violation, the entity: 1. contracted third-party company to create compliance program; 2. developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1; 3. designated a CIP Senior Manager; and 4. reviewed and obtained CIP Senior Manager Approval of the identified impact level. To prevent recurrence, the entity: 1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed
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 and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.

[redacted] NOC-2636 $10,000

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
NPCC2018020350	CIP-003-6	R1.1, R1.2	Medium	High	4/1/2017	9/4/2018	Self-Report	9/18/2018	5/24/2019

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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R1. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program. This violation started on April 1, 2017 when the entity failed to implement documented cyber security policies that address Cyber Security Awareness and Cyber Security Incident Response for its low impact BES Cyber System. The violation ended on September 4, 2018 when the entity's CIP Senior Manager reviewed and approved its CIP-003-6 Cyber Security – Security Management Controls policy. Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted].
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 the impact level of its assets and create and review one or more documented cyber security policies, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone. The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted].
Mitigation	To mitigate this violation, the entity: 1. contracted third-party to create compliance program; 2. implemented Cyber Security Awareness training; 3. implemented Cyber Security Incident Response Plan; 4. performed tabletop exercise of Cyber Security Incident Response Plan; and 5. created a facility specific CIP-003-6 procedure. To prevent recurrence, the entity: 1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed.
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 and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.

[redacted] NOC-2636 $10,000

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
NPCC2018020346	CIP-003-6	R2.	Lower	Severe	4/1/2017	9/4/2018	Self-Report	9/6/2018	5/24/2019

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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R2. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program. This violation started on April 1, 2017 when the entity failed to implement documented cyber security policies that address Cyber Security Awareness and Cyber Security Incident Response for its low impact BES Cyber System. The violation ended on September 4, 2018 when the entity implemented its approved CIP-003-6 Cyber Security – Security Management Controls policy. . Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. [redacted] did not have in place documented cyber security plans that addressed the sections in CIP-003-6 Attachment 1. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted].
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 the impact level of its assets and create and review one or more documented cyber security policies, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone. The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted].
Mitigation	To mitigate this violation, the entity: 1. Contracted third-party to create compliance program; 2. Implemented Cyber Security Awareness training; 3. Implemented Cyber Security Incident Response Plan; 4. Performed tabletop exercise of Cyber Security Incident Response Plan; and 5. Created a facility specific CIP-003-6 procedure. To prevent recurrence, the entity: 1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed
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 and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.

[redacted] NOC-2636 $10,000

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
NPCC2018020351	CIP-003-6	R3.	Medium	Severe	4/1/2017	9/4/2018	Self-Report	9/4/2018	12/12/2018

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 September 5, 2018, [redacted] (the entity) submitted a Self-Report stating that as a [redacted], it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R3. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program. This violation started on April 1, 2017 when the entity failed to identify a CIP Senior Manager by name. The violation ended on September 4, 2018 when the entity designated a CIP Senior Manager. Specifically, the facility in scope [redacted] the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations [redacted]. In particular, the entity did not incorporate amendments to the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed, assessed, or implemented when the entity [redacted].
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 a CIP Senior Manager the entity didn't have an individual responsible for ensuring compliance. As a result the entity failed to identify the impact level of its assets and failed to create and review one or more documented cyber security policies. By failing to implement these controls to ensure compliance, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to [redacted], if this connection were interrupted the entity would provide data to [redacted] via phone. The entity reduced the risk of its system becoming compromised by [redacted]. The Low Impact system is further protected from unauthorized physical access. [redacted].
Mitigation	To mitigate this violation, the entity: 1. identified and documented by name the CIP Senior Manager; 2. contracted third-party to create compliance program; and 3. created a facility specific CIP-003-6 procedure. To prevent recurrence, the entity: 1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed.
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 and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.

[redacted]

No penalty

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
WECC2018020039	CIP-004-3a	R3	Medium	High	8/6/2015 (when electronic access was provisioned without a PRA)	5/3/2018 (when a PRA was performed)	Self-Report	5/3/2018	4/3/2019

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 July 18, 2018, the entity submitted a Self-Report stating that, as a [redacted], it was in violation of CIP-004-3a R3. The entity conducted an internal audit beginning in October 2017, as part of mitigation related to two previous violations for the same Standard and Requirement and realized a gap in adherence to its procedures for ensuring that a Personnel Risk Assessment (PRA) was conducted for individuals authorized for electronic access to Critical Cyber Assets (CCAs). In January of 2018, the affected departments that utilize those access management procedures met to discuss and address the gap in adherence, with internal controls. While implementing one of the controls, the entity identified one employee who was authorized and granted electronic access on August 6, 2015 to software on a CCA, used for outage coordination, without first having a completed PRA for the person. Because the entity did not perform a PRA on the employee, they were not in the PRA tracking database, which the entity used to help reconcile employees with CIP electronic and physical access. The entity did not have any other controls in place within its processes to identify the issue sooner. On May 3, 2018, the entity performed the missing PRA for the one employee, for a total of 1,002 days of noncompliance. The root cause of this violation was the entity's personnel not following documented procedures, which required processing of CIP electronic access requests through the department that performed the PRAs, prior to the access being granted. After reviewing all relevant information, WECC determined the entity failed to conduct a PRA for one employee prior to granting electronic access to CCAs, as required by CIP-004-3a R3.
Risk Assessment	This violation posed a moderate 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 conduct a PRA for one employee prior to granting electronic access to CCAs, as required by CIP-004-3a R3. The entity had no internal controls implemented to detect or prevent this violation for nearly three years. Given the extent of the employee's access within the outage scheduling software, had they had malicious intent, they could have caused significant harm. However, the employee was authorized to have the electronic access and was sufficiently trained to use the software to perform their job. Additionally, the internal control, that was implemented in place as part of the mitigation of previous violations, identified the single individual that did not have the PRA in the tracking database. If there were any other individuals missing the PRA, this control would have identified it.
Mitigation	To mitigate this violation, the entity: 1) completed a PRA for the one employee in scope; 2) re-circulated its PRA verification procedure to applicable personnel; and 3) held a meeting with applicable personnel to discuss and train for the procedures and processes that need to be followed for compliance. During this meeting the attendees agreed that the [redacted] will verify PRAs with [redacted] if the personnel requesting access is new to their system. If the personnel is requesting additional access to an area, the [redacted] will verify access by checking the name against the PRA Audit SharePoint list maintained by [redacted]
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor The entity identified this violation utilizing an internal control it had implemented as part of the mitigation of a previous violation. [redacted] WECC considered the entity's CIP-004-3a R3 compliance history in determining the disposition track. WECC considered the entity's CIP-004-3a R3 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
WECC2018020282	CIP-006-3c	R4	Medium	Severe	[redacted] (when the first employee entered the PSP using a hard key)	8/30/2016 (when the ability to access the PSP utilizing a hard key was removed)	Self-Report	5/15/2017	10/4/2018

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 [redacted], WECC created a violation record for the entity, as a [redacted], for a violation of CIP-006-3c R4. The entity had increased the scope of an existing violation of CIP-006-6 R1, given NERC Violation ID [redacted], to include CIP-006-3c R4. WECC created the new violation record because the increase in scope had a start date of [redacted], which was before July 1, 2016, the mandatory and enforceable date of CIP Version 5.

Specifically, on [redacted], during a scheduled substation service power outage, which affected availability of the electronic access controls, the entity's employee was able to use a hard key to enter the control house Physical Security Perimeter (PSP) at a substation containing a Medium Impact BES Cyber System (MIBCS) with External Routable Connectivity (ERC). The door that was accessed had been designated to require the use of an alternate access key for entry to the PSP when electronic access controls failed or were out of service. Use of the alternate access key was intended to invoke the entity's procedure which required the Alarm Monitoring Station (AMS) to authenticate the person requesting access to the alternate access key, thus enforcing two-factor authentication per the entity's physical security plan. However, the door's key core had not been changed out to the alternate access key core required for MIBCS with ERC, per the established entity security standards, during the entity's NERC CIP V5 implementation efforts. Additionally, on August 9, 2016, another employee utilized an issued hard key to enter a control house PSP containing MIBCS with ERC. Similar to the issue mentioned above, the key core at this PSP door should have been switched out to comply with the entity's Alternate Access Key procedure which required two-factor authentication before access was permitted.

After reviewing all relevant information, WECC determined the entity failed to appropriately implement its documented operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R4.

The root cause of the violation was less than adequate internal controls. Specifically, the entity's CIP Version 5 project documentation did not incorporate a procedure to confirm all PSP door lock cores were replaced to comply with the entity's physical security plan.

This violation began on [redacted], when the first employee entered the PSP using a hard key, and ended on August 30, 2016, when the entity removed the ability to access the PSP through the alternate access door with the hard key, for a total of [redacted] days of noncompliance.

Risk Assessment

WECC determined this violation posed a minimal 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 appropriately implement its documented operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R4.

However, as compensation, the entity had a very limited the number of individuals with access to its PSPs and were only those who have a legitimate business need and who had completed Personnel Risk Assessments (PRAs) and CIP training. At the time of the violation the employees who accessed the PSPs were authorized to be there and had valid PRAs. No harm is known to have occurred.

Mitigation

To mitigate this violation, the entity:

1) changed the energized access key cores to the alternate access key cores at the two PSPs doors in scope;

2) conducted an audit on all alternate access key PSP doors containing MIBCS to ensure the core locks were appropriate. The entity identified six sites with key cores that were not set for utilization of alternate access keys. The entity mitigated by either installing the alternate access key cores or by inserting a non-key core lock and door handle to prohibit the door from being opened from the outside; and

	3) updated its physical security plans to include a test checklist as an internal control. The checklist requires that the tester attempt to use a specific key in all PSP door key cores and confirm that all other PSP doors have blank key cores.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor. [redacted] WECC considered the entity's CIP-006 -3c R4 compliance history in determining the disposition track and considered two previous violations to be an aggravating factor in the disposition determination. Additional compliance history related to CIP-006-6 R4 were not relevant because the associated violations were related to failing to maintain logs for physical access to PSPs; the entity's visitor control program; and its personnel risk assessment program, respectively, which involved different conduct than the violations in this disposition.

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
WECC2016015862	CIP-006-6	R1 P1.1,1.2, 1.3, and 1.4	Medium	Severe	[redacted]	7/19/2017 (when all issues were remediated)	Self-Report	11/14/2017	7/26/2018

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.)

On [redacted], the entity submitted a Self-Report stating that, as [redacted], it was in violation of CIP-006-6 R1. This noncompliance was identified by WECC auditors during the entity's CIP Version 3 to CIP Version 5 transitional audit on [redacted]. [redacted] WECC auditors provided the entity with an Area of Concern in accordance with guidance provided by NERC for CIP Version 5 transition audits. The entity then self-reported the noncompliance after receiving the audit report, knowing that the noncompliance was still occurring.

Specifically, several issues were identified with the implementation of CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4.

a. Regarding issue one (R1), the entity had a conference room located in its main building that was identified as a dual-purpose conference room that at times also functioned as a PSP. When not in use as a PSP, the entity did not ensure that all of the protective measures required in the Standards were applied.

b. Regarding issue two (R1 Part 1.1), the entity's Physical Access Control Systems (PACS) were protected by a PSP; however, the entity utilized mechanical locks and keys that were not managed with operational or procedural controls defined in its physical security plan.

c. Regarding issue three (R1 Part 1.2), the entity's employee identified [redacted] substations with an access door in the control house basement connected to a tunnel, designated as part of the PSP, that were found to have an emergency release (Safety) handle that did not require authentication for access into the PSP. The other end of the tunnel led to the outside. Entry by this manner was treated as an intrusion and would generate a response by security but did not require any type of authentication to gain access. The entity implemented this alternate path to comply with the National Fire Protection Association requirements for egress from the confined areas of the tunnel because the PSP space was concluded to be a necessary evacuation route.

d. Regarding issue four (R1 Part 1.3), the entity did not ensure a minimum of two-factor authentication to a PSP access point at the primary Control Center containing High Impact BES Cyber Systems (HIBCS). The management of the hard keys was not well documented and did not follow a two-factor authentication for use and distribution.

e. Regarding issue 5 (R1 Part 1.4), the entity did not implement continuous monitoring of windows, glass, and hatches for intrusion detection when PSP motion sensors were disabled, per its procedure, throughout the workday if one or more persons entered the PSP at six substations containing MIBCS. The disabling of the motion sensors also disabled intrusion monitoring through windows, glass, and some hatches at those substations. Specifically, on July 21, 2016, the entity received a loss of communication alarm from a PSP at a substation containing MIBCS with ERC. The entity's AMS operators notified Dispatch at the 15- and 30-minute marks concerning the loss of communications with the site; however, Dispatch did not direct and authorize human observation per the established procedures.

After reviewing all relevant information, WECC Enforcement determined the entity; 1) failed to define operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access; where technically feasible; 3) failed to utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for unauthorized access through a physical access point into a PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively.

The root cause of these violations was the lack of open and coordinated communication. Specifically, the different departments within the entity were not communicating or collaborating effectively during its implementation of Version 5 of the CIP Standards and Requirements.

	This violation began on [redacted] and ended on July 19, 2017, when the entity remediated all the issues, for a total of [redacted] days of noncompliance.
Risk Assessment	WECC determined these violations posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity, 1) failed to define operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access; 3) where technically feasible, failed to utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for unauthorized access through a physical access point into a PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively. However, the entity implemented good controls. All its PACS devices were within a designated PSP; the number of people with access to the PSPs was limited to those who had a legitimate need to access the area, and they all had PRAs. The PACS servers were monitored for unauthorized access. Additionally, the cabinets which housed the PACS control panels included tamper alarms, which would alert security officers if a cabinet were inappropriately accessed. The access tunnels were monitored around the clock, the use of the handle would have set off an alarm, and the tunnels are not accessible from the outside. Authentication, logging, and monitoring of physical access was captured for all individuals that entered the tunnel, which was the only way into the PSPs.
Mitigation	To mitigate CIP-006-6 R1 Part 1.1, the entity has: 1) developed a key control program for alternate access to PACS servers; 2) changed the field site location from a designated PSP to a secure area and updated documentation; 3) provided test results after the PACS system was moved to its new secure areas; and 4) provided guidance for applicable personnel for identifying the required security controls for a PACS system that resides within a PSP or outside of a PSP. To mitigate CIP-006-6 R1 Part 1.2, the entity has: 1) identified all sites containing MIBCS that utilize the pull handle safety device; 2) reviewed each site's tunnels and hatches for conformance to its physical security standards; 3) developed plans for sites that deviated from the physical security standard to bring the tunnels and hatches into compliance with its physical security standards; 4) reviewed all hatches and service doors to tunnels that are not a PSP access point to ensure they are locked down and cannot be opened from the exterior of the tunnel space; 5) ensured all tunnel doors into the PSP with the pull handle are monitored 24/7, and the use of the pull handle immediately generates a forced door event to the AMS; 6) tested that the alarms were working; and 7) updated the response procedure that the AMS operators use to investigate "Forced Door" alarms. The pull handles are documented on all PSP drawings, and AMS operators are trained to respond to all forced door events. To mitigate CIP-006-6 R1 Part 1.3, the entity has: 1) collected and inventoried all assigned keys to the primary Control Center; 2) developed and implemented a procedure for primary Control Center key control. The referenced operations bulletin was sent to AMS for their action, and the process was made available to employees; 3) updated the Physical Security Plan to change security responsibilities to security personnel and posted an operations bulletin that describes the processes to the Control Center employees; 4) assigned the PSP keys for the primary Control Center to Physical Security organization and stored them within a secure key box residing in the security AMS; 5) moved the key management program to the Physical Security organization; and 6) audited the updated procedure for effectiveness. To mitigate CIP-006-6 R1 Part 1.4, the entity has: 1) enhanced the training program and procedures between AMS and Dispatch to deploy resources for physical observation within the 30 minutes required by its Loss of Security System procedure; and

	2) implemented a script for contractors to read as part of their enhanced procedures between AMS and Dispatch.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor. [redacted] WECC considered the entity's CIP-006-6 R1 compliance history and determined there were no relevant instances of noncompliance.

[redacted] $80,000

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
WECC2017018174	CIP-006-3c	R1; R1.1	Medium	Severe	1/13/2012 (when the substation became a Critical Asset)	12/9/2016 (when the relays were disconnected from the ESP)	Self-Report	6/13/2018	11/1/2018

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 August 14, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation with CIP-006-3c R1.

Specifically, the entity reported that on June 4, 2015, it discovered that [redacted] that were part of an Electronic Security Perimeter (ESP) were located outside the designated Physical Security Perimeter (PSP) of a substation. The [redacted] were located in a [redacted], which was protected by the perimeter fence but outside the documented PSP. [redacted] of the [redacted] were used for Supervisory Control and Data Acquisition (SCADA) control between [redacted], and the other [redacted] were used for protection of [redacted] Although the entity identified the issue in 2015, it mistakenly marked the issue as remediated. On October 10, 2016, while performing a site validation assessment for CIP Version 5, the entity discovered that the [redacted] remained connected to the ESP and were still located outside the PSP.

After reviewing all relevant information, WECC Enforcement determined that the entity failed to ensure that all Cyber Assets within an ESP resided within an identified PSP, as required by CIP-006-3c R1.1.

The root cause of the violation was a less than adequate process. Specifically, the entity did not evaluate the ESP and PSP at the substation for compliance before or after it was energized.

WECC determined that this violation began on January 13, 2012, when the substation became a Critical Asset for CIP Version 3, and ended on December 9, 2016, when the [redacted] were disconnected from the ESP, for a total of 1,793 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 ensure that [redacted] Cyber Assets within an ESP resided within an identified PSP, as required by CIP-006-3c R1.1.

The entity implemented no preventive or detective controls as this violation was not discovered within a timely manner and only because the entity was implementing a newer version of the CIP Standards. Additionally, the entity had weak corrective controls as the violation was originally discovered in 2015, but marked as resolved and was not re-discovered until October of 2016. However, as compensation, [redacted]

Mitigation

To remediate and mitigate this violation, the entity:

1) removed the [redacted] from the ESP;
2) enhanced both of its work management ticketing systems to identify and track work at BES sites or with BES Cyber Systems;
3) updated its procedure to include instructions on what steps should be followed to add a new ESP, including which Cyber Assets should be included within the PSP;
4) updated its procedure to address its assessments for ESPs and PSPs; and
5) created and provided training for its updated processes and procedures to applicable personnel.

Other Factors

WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.

The entity did not receive mitigating credit for cooperation. The entity did not quickly address the violations, determine the facts, and report mitigation. This is evident by the duration between the Self-Report date and the Mitigation Plan submittal dates which was 403 days.

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-006-3c R1 compliance history in determining the penalty. WECC determined the entity's CIP-006-3c R1 compliance history to be an aggravating factor in the penalty determination.

[redacted] $80,000

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
WECC2017017885	CIP-005-5	R2; P2.3	Medium	Moderate	7/1/2016 (when the Standard and Requirement became enforceable)	4/4/2017 (when the entity modified the firewall access rules to the legacy device)	Self-Report	1/18/2019	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 June 30, 2017, the entity submitted a Self-Report stating that, as a [redacted], it was in violation with CIP-005-5 R2.

Specifically, the entity reported that while performing an internal controls assessment in February 2017, it discovered that [redacted] Information Technology (IT) cybersecurity personnel were using a legacy intermediate device (ID) for Interactive Remote Access (IRA), which did not require multi-factor authentication, to remotely access Protected Cyber Assets (PCAs) within various ESPs for [redacted] High Impact BES Cyber Systems (HIBCS) and [redacted] Medium Impact BES Cyber Systems (MIBCS). The entity had replaced this legacy ID with a new IRA system which did require multi-factor authentication. IT cybersecurity personnel had been instructed to utilize the new IRA system and stop using the legacy ID. However, because the entity had not removed the firewall rules that allowed remote access to the various ESPs through the use of the legacy ID, IT cybersecurity personnel continued to use the legacy ID Internet Protocol (IP) to connect to the various ESPs.

After reviewing all relevant information, WECC Enforcement determined the entity failed to require multi-factor authentication for all IRA sessions, as required by CIP-005-5 R2 Part 2.3.

The root cause of the violation was less than adequate internal controls and follow up. Specifically, the entity did not have controls in place to ensure that personnel were using the appropriate and authorized IRA system, and that firewall rules were such that they prevented access to the legacy device.

WECC determined that this violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on April 4, 2017, when the entity removed the firewall access rules from the source IP that allowed connection to the various ESPs, for a total of 278 days of noncompliance.

Risk Assessment

WECC determined that 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 require multi-factor authentication for all IRA sessions to access [redacted] HIBCS and [redacted] MIBCS, as required by CIP-005-5 R2 Part 2.3.

However, the entity implemented strong internal controls. Specifically, the entity [redacted]. These controls lowered the likelihood of a malicious actor gaining access.

Mitigation

To remediated and mitigate this violation, the entity:

1) removed user access to the ESPs from the unauthorized ID;
2) [redacted]
4) developed new rules to improve firewall management and tracking;
5) validated connectivity and created a process to ensure that when changing rules, they are correct;
6) verified successful explicit deny rule(s) for all admin traffic destined to ESP networks are working; and
7) implemented training of the new processes to all firewall administrators.

Other Factors

WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.

The entity did not receive mitigating credit for cooperation. The entity did not quickly address the violations, determine the facts, and report mitigation. This is evident by the duration between the Self-Report date and the Mitigation Plan submittal date, which was 441 days.

[redacted] $80,000

	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-005-5 R2 compliance history in determining the penalty. WECC determined the entity's CIP-005-5 R2 compliance history to be an aggravating factor in the penalty determination.

[redacted] $74,000

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
WECC2018019006	CIP-005-5	R1; P1.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity)	4/3/2017 (when the reason for granting access was properly documented)	Self-Report	4/4/2018	5/11/2018

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 19, 2018, the entity submitted a Self-Report stating that, as a [redacted] it was in violation of CIP-005-5 R1. Specifically, on April 3, 2017, while working on Transient Cyber Asset Access Control Lists (ACLs), the entity discovered that the reasons for granting access for five access rules were missing in the ACLs for [redacted] Electronic Access Points (EAPs) to the Electronic Security Perimeters (ESPs) of [redacted] different Medium Impact BES Cyber Systems (MIBCS) at [redacted] switching stations. Upon discovery, the entity added the appropriate reasons for granting access to the ACLs on the [redacted] EAPs and saved the [redacted] EAP configurations, therefore remediating the possible violation on the same day it was discovered. After reviewing all relevant information, WECC determined the entity failed to include the reason for granting access for inbound and outbound access permissions, for [redacted] EAPs as required by CIP-005-5 R1, Part 1.3. The root cause of the violation was a lack of written communication. Specifically, the task to review all ACLs and ensure the reason for granting access was properly documented; however, it was not part of the entity's CIP Version 5 transition project plan. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable on the entity, and ended on April 3, 2017, when the entity properly documented the reason for granting access within each ACL rule on the [redacted] EAPs in scope, for a total of 276 days of noncompliance.
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, the entity failed to include the reason for granting access for inbound and outbound access permissions, for two EAPs as required by CIP-005-5 R1, Part 1.3. This violation was a documentation issue rather than technical in nature. The entity implemented strong controls. Specifically, its network was implemented with "hub and spoke" technology in that another Cyber Asset was in place between the EAPs in scope and the external network, which had its ACL rules set to block traffic not permitted, with access comments for granting other permitted access. This setup increased the security posture and provided defense in depth. The [redacted] EAPs in scope were also configured to block all traffic.
Mitigation	To mitigate this violation, the entity has: 1) added reasons to each of the ACLs on [redacted] the EAPs and saved the two EAP configurations; 2) created a Security Information and Event Management (SIEM) policy test that will run daily, verify that all ACLs have a comment, and send results weekly to applicable personnel; 3) updated the CIP-005-5 procedure document to include peer review of ACLs and to ensure that comments are added to all ACLs when a new ACL is added, updated, or changed; and 4) sent an email to the applicable personnel to notify them of the new peer review process.
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's ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it involved conduct distinct from this violation. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning 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
WECC2017016941	CIP-005-5	R1; P1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	7/14/2016 (when malicious communication detection was reestablished)	Self-Report	5/23/2018	8/22/2018

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 February 6, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-005-5 R1. On July 7, 2016, the entity discovered, via an automated alert from the management console, that there was a configuration issue with [redacted] Cyber Asset pairs ([redacted] devices) configured in high availability fail-over configuration mode. These Cyber Assets were classified as EAPs to the ESP protecting the High Impact BES Cyber Systems (HIBCS). Upon further investigation, the entity determined that during its transition to CIP Version 5, a critical configuration setting was missed in the Intrusion Detection System (IDS) module for each of the [redacted] EAPs pairs. All configuration for the IDS modules had been completed as of July 1, 2016 except for a single configuration setting. Because of the missing IDS module configuration setting, the EAPs did not have a method for detecting known or suspected malicious communications for both inbound and outbound communications from July 1, 2016 to July 14, 2016, when the entity added the configuration settings. After reviewing all relevant information, WECC determined that the entity failed to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, as required by CIP-005-5 R1 Part 1.5. The root cause of the violation was less than adequate controls for verifying configuration settings on the three EAP pairs during the NERC CIP Version 3 to Version 5 transition. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on July 14, 2016, when malicious communication detection was reestablished, for a total of 14 days of noncompliance.
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, the entity failed to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, as required by CIP-005-5 R1 Part 1.5. However, the entity implemented strong controls. Specifically, the entity utilized a SIEM to detect changes in the configuration of devices and included commands to ensure raw data was analyzed and alerted on actionable information. [redacted]. The entity discovered this noncompliance as a result of investigating the alerts. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets. [redacted]
Mitigation	To mitigate this violation the entity: 1) added the missing IDS module configuration to the [redacted] EAP pairs; 2) reseated the cable into the sensor port; 3) created a SIEM policy test to monitor and detect for changes; 4) provided training for the EAP with sensor port services; 5) upgraded the software level on the [redacted] affected EAPs active/standby pairs; and 6) held a mitigation closure meeting with applicable personnel related to all compliance elements of CIP-005-5 R1.
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's ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it involved conduct distinct from this violation.

[redacted] NOC-2635 $74,000

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
WECC2017016941	CIP-005-5	R1; P1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	7/14/2016 (when malicious communication detection was reestablished)	Self-Report	5/23/2018	8/22/2018
			WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.						

[redacted] NOC-2635 $74,000

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
WECC2017016928	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	12/19/2018 (Mitigation Plan completion)	Self-Report	12/19/2018	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 February 3, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R2.

Specifically, for the entity's patch management process for tracking, evaluating, and installing cyber security patches pursuant to CIP-007-6 R2 Part 2.1, it utilized a configuration management application to maintain a comprehensive software whitelist. The whitelist was intended to track all software and the associated security patch sources installed on all [redacted] HIBCS and MIBCS BCAs, and the associated Electronic Access Control and Monitoring System (EACMS), Physical Access Control System (PACS), and Protected Cyber Assets (PCAs). The software whitelist was utilized as the starting point to execute CIP-007-6 R2 Part 2.1 through Part 2.4. On November 3, 2016, during the entity's efforts to true-up its software whitelist to the actual installed software on all its HIBCS and MIBCS BCAs and associated EACMS, PACS, and PCAs, it was discovered that several software applications on [redacted] HIBCS BCA, [redacted] EACMS associated with the HIBCS and [redacted] PCAs associated with [redacted] separate MIBCS, were not originally captured in the software whitelist during the CIP Version 5 implementation effort. Additionally, on December 13, 2016, and February 2, 2017, during continued efforts to true-up its software whitelist, the entity discovered another software application installed on [redacted] HIBCS BCAs, [redacted] PCAs and [redacted] EACMS associated with the HIBCS, as well as [redacted] HIBCS BCAs, respectively, where the software and the associated patch sources were missing from the software whitelist. None of this software was being tracked for cyber security patches, therefore the patches were not being evaluated, applied, or had mitigation plans created. This issue affected [redacted] BCAs ([redacted] in HIBCS and [redacted] in MIBCS), [redacted] EACMS, [redacted] PCAs and [redacted] PACS associated with the HIBCS, as well as [redacted] EACMS and [redacted] PCAs associated with the MIBCS, for a total of [redacted] Cyber Assets.

After reviewing all relevant information, WECC determined the entity failed to identify a source or sources to track for the release of cyber security patches for applicable Cyber Assets that were updateable and for which a patching source exists, for [redacted] applicable Cyber Assets, as required by CIP-007-6 R2 Part 2.1. As a result, the entity also failed to evaluate security patches for applicability for the software applications installed on those [redacted] devices, as required by CIP-007-6 R2 Part 2.2; as well as failed to take action for [redacted] patches to either apply the patches, or create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.

The root cause of the violation was management policy guidance or expectations not being well-defined, understood, or enforced. Specifically, the entity had no project plans in place to address this requirement, the scope of the tasks was unknown, and available resources were constrained. Additionally, there was a misalignment of the operations team's skill sets and resource assignment.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended when the entity completed its mitigation plan on December 19, 2018, for a total of 902 days of noncompliance.

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, the entity failed to identify a source or sources to track for the release of cyber security patches for applicable Cyber Assets that were updateable and for which a patching source exists, as required by CIP-007-6 R2 Part 2.1. As a result, the entity also failed to evaluate security patches for applicability for the software applications installed on those Cyber Assets, as required by CIP-007-6 R2 Part 2.2; as well as failed to take action for applicable patches to either apply the patches, or create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.

However, the entity had implemented strong controls. None of the affected Cyber Assets were internet-facing. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets. [redacted]

Mitigation

To mitigate this violation, the entity:

1) inventoried all installed software applications utilizing its SIEM reporting tool, and added any missing installed software applications to asset management tool software;
2) used a whitelist to ensure that all installed software applications are added to and being tracked in the vulnerability management service where possible;
3) inventoried all installed firmware and added to the vulnerability management service for tracking and evaluation of firmware in its environment;
4) uninstalled software applications that are no longer needed and removed them from the software whitelist;

[redacted] $74,000

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
WECC2017016928	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	12/19/2018 (Mitigation Plan completion)	Self-Report	12/19/2018	TBD

	5) updated the SIEM [redacted] functions to ensure use of the best reporting tools available from the SIEM; 6) inspected the software whitelist entries for inclusion and exclusion errors that could cause software to be excluded from the evaluation work flow; 7) added functionality to its asset management tool to make it apparent to a user that an entry is either including or excluding software from the whitelist; 8) developed and documented a process for the evaluation of software and firmware entries in the software whitelist that are not able to be tracked by vulnerability management service; and 9) held training for subject matter experts (SMEs) responsible for evaluating software and firmware patches.
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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. WECC considered the entity's CIP-007-6 R2 compliance history in determining the penalty. WECC determined the entity's CIP-007-6 R2 compliance history to be an aggravating factor in the penalty determination. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.

[redacted] $74,000

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
WECC2017016939	CIP-007-6	R3; P3.1	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	5/19/2017 (when the physical ports were locked and added antivirus to the PCA)	Self-Report	4/10/2018	10/11/2018

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 February 6, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-007-6 R3.

Specifically, the entity utilized physical port locking as one of the methods to deter, detect, or prevent malicious code on it CIP applicable Cyber Assets. However, on January 19, 2017, the entity identified that [redacted] ports on [redacted] MIBCS BCAs without External Routable Connectivity (ERC) had not been port locked as of July 1, 2016. The employee responsible for this task mistakenly applied the CIP-007-6 R1, Part 1.1 methodology of leaving the physical ports instead of the logical ports open. Upon identification of the missing port locks, the entity began the process of physically port locking [redacted] ports on [redacted] of the BCAs, which was completed on February 10, 2017. The entity did not physically port lock one port each on the [redacted] remaining BCAs because it was in the process of decommissioning those devices, which it completed on December 13, 2016. Additionally, [redacted] PCA did not have antivirus installed as required by CIP-007-6 R3 Part R3.1.

After reviewing all relevant information, WECC determined the entity failed to deploy methods to deter, detect, or prevent malicious code on [redacted] MIBCS BCAs without ERC and [redacted] PCA, as required by CIP-007-6 R3 Part 3.1.

The root cause of the violation was not understanding the documented processes. Specifically, an employee mistakenly applied the CIP-007-6 R1, Part 1.1 methodology of leaving the physical ports instead of logical ports open on the BCAs in scope.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 19, 2017, when the entity physically port locked the remaining BCAs in scope and added antivirus to the PCA, for a total of 322 days of noncompliance.

Risk Assessment

This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The entity failed to deploy methods to deter, detect, or prevent malicious code on [redacted] MIBCS BCAs without ERC, as required by CIP-007-6 R3 Part 3.1.

However, the entity implemented an extensive SIEM architecture that continually monitors changes on HIBCS and MIBCS Cyber Assets and alerts the operations group of unauthorized changes. The SIEM also monitors network switch configurations to ensure enabled ports have a description entered. [redacted] This protection is provided for all devices on the network segment, including those without the anti-malware software installed. [redacted]

Mitigation

To mitigate this violation, the entity:

1) placed tamper tape on open ports on [redacted] of the BCAs in scope;
2) implemented a mandatory escort checklist to ensure the responsibilities of authorized escorts are met and to identify any potential incidents, including physical disturbances such as broken tamper tape or missing port locks. The checklist will also outline the proper response steps to be taken in the event an incident/disturbance is discovered;
3) documented a process to capture cyber security controls for all new cyber assets and/or new device types at transmission facilities to prevent introducing any device types that could create a CIP or Reliability risk;
4) decommissioned the remaining [redacted] BCAs in scope;
5) installed antivirus on applicable devices;
6) removed legacy non-ERC device types associated with its MIBCS which were classified as BCA and replaced them with devices capable of ERC;
7) communicated to applicable personnel new process changes;
8) reviewed and/or edited procedure to ensure full understanding of the documented controls to prevent malicious code on non-ERC devices; and
9) ensured that reports from the antivirus software were created, scheduled, and being sent to appropriate personnel for their review and verification that antivirus was installed on all applicable devices.

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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.

[redacted] NOC-2635 $74,000

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
WECC2017016939	CIP-007-6	R3; P3.1	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	5/19/2017 (when the physical ports were locked and added antivirus to the PCA)	Self-Report	4/10/2018	10/11/2018
			The entity received mitigating credit for admitting to the violation. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it was distinct, separate, and not relevant to this violation. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning 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
WECC2017016938	CIP-007-6	R4; P4.2.2	Medium	High	11/8/2016 (when the SIEM stopped functioning correctly)	12/26/2016 (when the SIEM began logging and alerting for events)	Self-Report	5/17/2018	10/11/2018

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 February 6, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R4.

Specifically, on December 7, 2016 during a log review, the entity identified a potential logging issue with its SIEM, the event logging and alerting tool utilized to perform CIP-007-6 R4 for its HIBCS and MIBCS and the associated EACMS, PCAs, and PACS, as applicable, for technically capable devices. As a result, the entity worked with the SIEM vendor to determine that the SIEM database had been corrupted since November 8, 2016. Subsequently, the entity rebuilt the indexes in the database and brought the SIEM back to a normal operating state by December 26, 2016. During the 48-day span while the SIEM database was not operating correctly, [redacted] Cyber Assets were not reporting to the SIEM: [redacted] BCAs, [redacted] EACMS devices, [redacted] PCAs, and [redacted] PACS Cyber Asset, all associated with the HIBCS, and [redacted] PCAs associated with the MIBCS. The identified Cyber Assets were still logging locally, therefore once the SIEM database was repaired, all data was able to be restored and captured for the 48-day timeframe. Furthermore, the antivirus continued to function as expected during this timeframe and could send its logs to the antivirus policy administrator console, which was capable of alerting on malicious code. However, during the 48-day span, the [redacted] Cyber Assets were not able to send logs to the SIEM in order for the SIEM to generate alerts for a detected failure of Part 4.1 event logging. Because all logs were cached on the local devices, when the SIEM became operational again, all logs were forwarded on, normalized, and correlated. Any logs that would have caused an alert from the SIEM would have been sent when the SIEM was repaired.

Additionally, the entity reported that as a result of the issue with the SIEM, the [redacted] Cyber Assets associated with its HIBCS were not included in the 15-calendar day log review during the 48 days in which the SIEM database was not operating correctly.

After reviewing all relevant information, WECC determined the entity failed to generate alerts for detected failure of Part 4.1 event logging, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2. WECC also determined that the entity did not violate CIP-007-6 R4 Part 4.4 because logs were being reviewed at a summary level as required.

The root cause of the violation was an equipment malfunction. Specifically, the entity's SIEM, which is its event logging and alerting tool, experienced a corruption of its database.

This violation began on November 8, 2016, when the SIEM stopped functioning correctly, and ended on December 26, 2016, when the SIEM began logging and alerting for events, for a total of 48 days of noncompliance.

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, the entity failed to generate alerts for detected failure of Part 4.1 event logging, as required by CIP-007-6 R4 Part 4.2 Sub-Part 4.2.2.

However, the entity implemented strong controls. The risk of malicious code was mitigated by the entity's implementation of antivirus since it has the ability to log and alert. The risk of loss of logs on the Cyber Assets was mitigated, as the information was cached and sent to the SIEM upon re-indexing of the database. All Cyber Assets in question were protected within Physical Security Perimeters (PSPs) which was verified at audit. The antivirus continued to function as expected during this timeframe and could send its logs to the antivirus policy administrator console, which was capable of alerting on malicious code. Additionally, the entity implemented task reminders to remind employees to review logs which included escalations up to senior management if the task is not completed prior to the due date. While performing the manual review of those logs, this noncompliance was identified.

Mitigation

To mitigate this violation the entity:

1) corrected the SIEM database corruption;
2) verified that the SIEM database was operational and ensured that all logs were normalized and reporting--no database corruption errors were displayed in the console manager log;
3) updated the CIP-007-6 R4 procedure regarding log review;
4) created a SIEM Normal Operations Dashboard that will exhibit the health and normal operations of the SIEM by utilizing dynamic insights of critical components of the SIEM;
5) conducted a summary review of logs from July 1, 2016 to the date the database indexes were rebuilt to ensure no potential Cyber Security Incidents went undetected. The logs were restored, and a representative sample was used for the review;
6) updated the CIP-007-6 R4 procedure to include all the new processes; and
7) provided training to applicable personnel on the updated CIP-007-6 R4 procedures.

[redacted] NOC-2635 $74,000

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
WECC2017016938	CIP-007-6	R4; P4.2.2	Medium	High	11/8/2016 (when the SIEM stopped functioning correctly)	12/26/2016 (when the SIEM began logging and alerting for events)	Self-Report	5/17/2018	10/11/2018
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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. WECC considered the entity's CIP-007-6 R4 compliance history in determining the penalty. WECC determined the entity's CIP-007-6 R4 compliance history to be an aggravating factor in the penalty determination. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.								

[redacted] $74,000

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
WECC2017016940	CIP-007-6	R5; P5.5.1, P5.5.2	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	1/25/2017 (when password parameters were set for the accounts)	Self-Report	10/19/2018	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 February 6, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-007-6 R5.

Specifically, on December 9, 2016, while the entity's engineers were executing its change management process to install new MIBCS BCAs at a switching station, the entity's Operations SMEs provided temporary passwords for the BCAs to be functionally tested prior to their deployment into the ESP where the BCA password length and complexity would be automatically enforced via a substation remote access system. Upon the Operations SMEs providing the temporary passwords, the [redacted] SMEs identified that both the temporary passwords and the enforcement of password length and complexity in the substation remote access system for these particular BCAs did not meet the minimum password parameters as required by Part 5 Sub-Part 5.5.1 (length) and Part 5 Sub-Part 5.5.2 (complexity), even though the substation remote access system and the BCAs could support such parameters. Upon discovery, it was determined that the Operations SMEs would enforce password length and complexity procedurally until the scope of the potential issue could be determined and corrected in the substation remote access system.

Upon further investigation, the entity determined that [redacted] BCAs and [redacted] EACMS Cyber Assets associated with the MIBCSs at [redacted] switching stations did not have the appropriate CIP-007-6 R5.5 password parameters in place. The [redacted] Cyber Assets were identified as not meeting either one or two of the Sub-Parts of CIP-007-6 R5 Part 5.5, which equated to [redacted] accounts with passwords that needed to be changed, out of a total population of [redacted] accounts with passwords managed by the substation remote access system. As of January 25, 2017, all [redacted] passwords for the [redacted] Cyber Assets had been updated to meet length and complexity requirements, and all password settings within the substation remote access system had been corrected to meet CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.

After reviewing all relevant information, WECC determined the entity failed to implement a process for password-only authentication for interactive user access, either technically or procedurally, and to enforce password parameters 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 a lack of internal controls during the entity's transition from Version 3 to Version 5. Specifically, there was insufficient run time in the entity's project plan to validate the configuration prior to the effective date of Version 5. During this time, the entity was implementing a new change management system and did not allow configuration changes, other than for emergencies, to CIP Cyber Assets. Had the entity's change management been in place at the time, it would have likely caught the misconfiguration.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on January 25, 2017, when password parameters were set for the accounts to the devices in scope, for a total of 209 days of noncompliance.

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, the entity failed to implement a process for password-only authentication for interactive user access, either technically or procedurally, and to enforce password parameters, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.

However, the entity implemented strong controls. [redacted]

Therefore, while password length and complexity did not meet the CIP-007-6 R 5 Part 5.5 length and complexity requirements between July 1, 2016 and January 25, 2017, password enforcement was still set to a minimum length of five characters or more (depending on the device type) and a minimum complexity of two different character types during the violation duration.

Mitigation

To mitigate this violation, the entity:

1) updated the passwords associated with the identified Cyber Assets to meet length and complexity requirements;
2) update the SIEM policy test to ensure it shows that the passwords for devices in scope meet the parameters of CIP-007 R5 Part 5.5;
3) created a tool to assist in identifying CIP requirements, if any, that apply to new devices prior to approval of any final design that is planned to go through the entity's commissioning process;
4) documented a process to capture Cyber Security controls for all new Cyber Assets prior to any commissioning of a Cyber Asset;
5) ensured business unit procedures align to support password length and complexity for any new devices coming online; and

[redacted] $74,000

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
WECC2017016940	CIP-007-6	R5; P5.5.1, P5.5.2	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	1/25/2017 (when password parameters were set for the accounts)	Self-Report	10/19/2018	TBD
			6) held a mitigation closure meeting with all mitigation SME team members, as well a representative from [redacted] management, applicable Operations SMEs, and its [redacted] Completed remediation and mitigation tasks and procedures will be discussed, reviewed, and verified.						
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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it was distinct, separate, and not relevant to this violation. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.						

[redacted] $74,000

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
WECC2017016926	CIP-010-2	R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	5/1/2017 (when baseline configurations were developed and captured)	Self-Report	3/29/2019	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 [redacted] the entity submitted a Self-Report stating, as a [redacted] it was in violation of CIP-010-2 R1.

Specifically, on August 4, 2016, during its first performance of a bookend review of CIP-010-2 R2 Part 2.1 baseline configurations, the entity's [redacted] SMEs became concerned that some baseline elements might be missing from some Cyber Asset baseline configuration details. At the time, the entity believed that it may not have complete baseline configurations captured for only a few Cyber Assets since port scanning could not be accomplished due to connectivity problems between its configuration monitoring tool and the Cyber Assets. However, to examine the scope of the issue, and to perform the necessary due diligence, [redacted] began an effort on August 25, 2016 to review each Cyber Asset in its Cyber Asset inventory to ensure that all required and applicable CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1 through 1.1.5 baseline elements were captured for each applicable Cyber Asset. The entity concluded that the scope of this violation included [redacted] Cyber Assets ([redacted] BCAs, [redacted] EACMS, and [redacted] PCAs) at the HIBCS and MIBCS. During the entity's [redacted] audit, WECC auditors confirmed an additional [redacted] Cyber Assets ([redacted] BCAs, [redacted] EACMS, and [redacted] PCAs) as being in scope of this violation, for a total of [redacted] Cyber Assets, along with the baseline element that was missing from the Cyber Assets baseline configuration. [redacted] of the [redacted] Cyber Assets were in violation of sub-part 1.1.1; [redacted] were in violation of sub-part 1.1.2; [redacted] were in violation of sub-part 1.1.4; and [redacted] was in violation of sub-part 1.1.5.

After reviewing all relevant information, WECC determined the entity failed to develop a baseline configuration individually or by a group, as required by CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1, 1.1.2, 1.1.4, and 1.1.5.

The root cause of the violation was less than adequate procedures. Specifically, the entity had a procedure in place to meet objectives of the Requirements; however, the procedure did not contain complete and accurate information to meet those objectives. Additionally, the entity had no procedure in place to address configuration and communication issues with the SIEM.

This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 1, 2017, when baseline configurations were developed and captured for the Cyber Assets in scope, for a total of 305 days of noncompliance.

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, the entity failed to develop a baseline configuration individually or by a group, as required by CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1, 1.1.2, 1.1.4 and 1.1.5.

However, the entity implemented strong detective controls. [redacted] The entity did not implement controls to prevent this violation from occurring but did employ detective controls which identified the violation. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets.

Mitigation

To mitigate this violation, the entity has:

1) collected the number and names of devices missing baseline elements and completed baseline configurations on the Cyber Assets in scope;
2) documented a process to capture cyber security controls for all new Cyber Assets and/or new device types at Transmission facilities to prevent introducing any device type that could create a CIP or Reliability risk;
3) upgraded applicable configuration monitoring tool device profilers to compatible firmware versions to ensure automated port scan capability;
4) provided training to SMEs on SIEM admin, security, and compliance;
5) for any baselines that are being tracked manually (e.g. in spreadsheets), converted to Offline Device Type in its asset management system in order for the baseline element to be documented within the configuration monitoring tool. An alternative is to track the baseline element through configuration monitoring tool scanning if possible. The desired end result is that all baseline documentation resides within the configuration monitoring tool;
6) promoted all 'unpromoted changes', which will set the as-is device state to be the current baseline;
7) updated baseline reports to include only the required information to help SMEs more easily see if/when information is missing;

[redacted] $74,000

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
WECC2017016926	CIP-010-2	R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	5/1/2017 (when baseline configurations were developed and captured)	Self-Report	3/29/2019	TBD

	8) updated the CIP-010-2 R1 procedure to reflect the changes to processes, documentation, and reporting that have been made, to include updating procedures for how to commission offline devices that includes a process for adding manual baseline configurations into its asset management system; and 9) trained applicable personnel on commissioning new CIP devices to ensure clarity on the procedure of collecting and documenting baseline data.
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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date. WECC considered the entity's CIP-010-2 R1 compliance history in determining the penalty. WECC determined the entity's CIP-010-2 R1 compliance history to be an aggravating factor in the penalty determination. WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning 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
WECC2017016929	CIP-010-2	R2; P2.1	Medium	Severe	8/6/2016 (when baseline changes were not monitored)	11/11/2017 (when baseline changes commenced)	Self-Report	6/5/2018	10/11/2018

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 February 3, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in violation of CIP-010-2 R2. Specifically, on November 1, 2016, the entity's [redacted] SMEs discovered a misconfiguration within its configuration monitoring tool used to monitor the entity's Cyber Asset baseline configurations, which caused an EACMS associated with the HIBCS not to have its baseline configuration monitored from August 6, 2016 to November 1, 2016, as required by CIP-010-2 R2 Part 2.1. During the entity's investigation, to ensure other Cyber Assets did not have similar issues, it discovered [redacted] additional Cyber Assets where baseline configurations were not being monitored at least once every 35 calendar days for changes, from August 6, 2016 to January 26, 2017. The [redacted] Cyber Assets included [redacted] BCAs, in addition to [redacted] EACMS and [redacted] PCAs associated with the HIBCS. 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, as well as document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1. The root cause of the violation was less than adequate procedures. Specifically, the entity had a procedure in place to meet objectives of the Requirements; however, the procedure did not contain complete and accurate information to meet those objectives. Additionally, the entity had no procedure in place to address the configuration and communication issues with the SEIM. This violation began on August 6, 2016, when changes to baseline configurations were not being monitored, and ended on May 11, 2017, when monitoring of changes to baseline configurations commenced on the Cyber Assets in scope, for a total of 279 days of noncompliance.
Risk Assessment	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, as well as document and investigate detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1. However, the entity implemented strong controls. Specifically, the entity implemented an asset management system, which is used for off-line device management to facilitate a method to collect configuration information for Cyber Assets when it is difficult to implement technical or other controls. The information is gathered manually from the Cyber Assets in question and entered into the asset management system. Additionally, the risk specific to [redacted] of the BCAs in scope of this noncompliance was further reduced because changes to their baseline configurations could only be made through a physical hardware change, and not remotely.
Mitigation	To mitigate this violation, the entity: 1) worked with its SIEM vendor to develop and implement a solution that tracks the number of days since an asset was last monitored by the SIEM to verify successful baseline monitoring of Cyber Assets for a 35-day rolling window; 2) implemented new configuration monitoring tool rules, policy tests, and reports; 3) monitored the 20 Cyber Assets for baseline configuration changes; 4) created a daily automated test to run for Cyber Assets which do not directly connect to the SIEM to ensure that manual baseline checks are performed at least once every 35 calendar days. For those Cyber Assets that exceed a 35-day baseline monitoring check, a policy test will fail and the failure will be reflected on a daily email report sent to [redacted] 5) upgraded applicable configuration monitoring tool device profilers to compatible firmware versions to ensure automated port scan capability; 6) established an interface with the asset management functionality and collected the date the offline device type was last checked and used the new rules to calculate how long since the last check; 7) added the offline device type assets to the new configuration monitoring tool reports to report on failing assets; 8) updated the CIP-010-2 R2 procedure to reflect the changes to processes, documentation, and reporting that have been made as a result of the new reporting evidence; and 9) provided training to applicable personnel on the updated procedure.
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 ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date. WECC considered the entity's CIP-010-2 R2 compliance history in determining the penalty. WECC determined the entity's CIP-010-2 R2 compliance history to be an aggravating factor in the penalty determination.

[redacted] NOC-2635 $74,000

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
WECC2017016929	CIP-010-2	R2; P2.1	Medium	Severe	8/6/2016 (when baseline changes were not monitored)	11/11/2017 (when baseline changes commenced)	Self-Report	6/5/2018	10/11/2018
			WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over $50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.						

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														

[redacted] NOC-2627 $0

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.

[redacted] NOC-2627 $0

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.

[redacted] NOC-2627 $0

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.

[redacted] NOC-2627 $0

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.								

[redacted] NOC-2627 $0

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.

[redacted] NOC -2627 $0

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.

[redacted] NOC -2627 $0

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.						

[redacted] NOC -2627 $0

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.

[redacted] NOC -2627 $0

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.								

[redacted] NOC -2627 $0

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.

[redacted] $87,000

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.

[redacted] $87,000

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.

[redacted] $87,000

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.

[redacted] $87,000

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.

[redacted] $87,000

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.

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

[redacted] – [redacted] NOC-2612 No Penalty

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]

[redacted]		NOC-2612	No Penalty
	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.		

[redacted] NOC-2593 $0

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.

[redacted] NOC-2593 $0

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.

[redacted]	NOC-2593	$0

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.

[redacted] NOC-2593 $0

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.

[redacted] NOC-2593 $0

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.

[redacted] NOC-2593 $0

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.

[redacted] NOC-2593 $0

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.

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 filing 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	FRCC2018019002			Yes	Yes								Yes	Category 2 – 12: 2 years
2	FRCC2018019016	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
3	SPP2017018137			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year
4														
5														
6														
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														
37														

Filing Date: February 28, 2019

[redacted] – [redacted] NOC-2607 $0

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
FRCC2018019002	CIP-007-6	R2; P2.2	Medium	Severe	3/23/2017 (the day after the previous mitigation plan was completed)	3/5/2018 (when patches were evaluated and completed)	Spot Check	3/31/2018	8/10/2018

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 Spot Check conducted from January 15, 2018 through January 19, 2018, FRCC determined that the Entity, [redacted], was in noncompliance with CIP-007-6 R2 (Part 2.2). This noncompliance started on March 23, 2017, when the Entity failed to evaluate its security patches for applicability at least once every 35 calendar days on 12 out of 29 (41.4%) Cyber Assets (CA). The noncompliance ended March 5, 2018 when patches were evaluated and completed. The missed patches were for four (4) Energy Management System (EMS) servers, five (5) operator workstations within the EMS network, one (1) PACS server, and two (2) Programmable Local Access Control Panels. Although every patch was not critical, there were critical patches that missed the 35-day installation window. These missed patches could have prolonged the presence of software vulnerabilities, which, if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets. Although the patches in question did not meet the 35-day requirement, they were being installed on a quarterly basis. The entity did perform a vulnerability review and determined that during the time when the available security patches were not evaluated and applied as required, there were no known instances of unauthorized access or breaches to the entity's BES Cyber Systems and their associated EACMS, PACS, and PCAs. Specifically, the Entity CAs were being monitored by three external vendors. For all nine (9) of the CAs managed by External Vendor #2 and three (3) out of five (5) CAs managed by External Vendor #3, the Entity failed to 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 as required by CIP-007-6 (R2.2). The root cause was multiple vendors responsible for patching on different segments (Supervisory Control and Data Acquisition (SCADA), non-SCADA) of the Entity CAs and a lack of the Entity oversight.
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). Specifically, the Entity's failure to execute their patch management process could have prolonged the presence of software vulnerabilities, which if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets impacting the reliability of the BPS. The risk was reduced because all the devices were protected by a Physical Security Perimeter and all the Cyber Assets were within the Electronic Security Perimeter. In addition, Vendor #3 was completing the assessments quarterly instead of every 35 days. No harm is known to have occurred.
Mitigation	To mitigate this violation, the Entity: 1) evaluated and applied all security patches; 2) designated a single vendor (Vendor #1) to monitor for all newly released security patches 3) verified with Vendor #2 their responsibility to apply security patches on monthly basis; 4) developed internal control to ensure evaluation and application of Vendor #2 security patches; 5) developed situational awareness internal control to ensure SME applies security patches, including: - set-up an email from HelpDesk to Vendor #1 SME as a reminder to coordinate patching that needs to be completed for all vendors - set-up an email from HelpDesk informing the Entity SME that patching due date is approaching; and 6) trained all applicable personnel on new processes and/or procedures.
Other Factors	FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty. FRCC reviewed the Entity's compliance history and determined there was a relevant instance of noncompliance, which is considered to be aggravating. The previous extent of condition and gap

[redacted] – [redacted] NOC-2607 $0

	assessment of [redacted] appeared to be complete, however the mitigation only addressed Vendor #1. Subsequent issues were discovered with Vendors #2 and #3 that were not addressed by the previous mitigation plan. The current instance was discovered as part of a follow up Spot Check of [redacted]. FRCC resolved this noncompliance in an SNOP as aggravation for the previous noncompliance.

[redacted] – [redacted] NOC-2607 $0

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
FRCC2018019016	CIP-007-6	R5: P5.6; 5.7	Medium	Severe	7/1/2016 (when the Entity failed to enforce password changes and limit unsuccessful authentication attempts or generate alerts)	1/24/2018 (when the Entity corrected the patching issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel)	Spot Check	6/1/2018	8/10/2018

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 Spot Check conducted from January 15, 2018 through January 19, 2018, FRCC determined that the Entity, [redacted], was in noncompliance with CIP-007-6 R5 (Parts 5.6 & 5.7). This noncompliance started when the Standard became mandatory and enforceable on July 1, 2016, when the Entity failed to enforce password changes, and limit unsuccessful authentication attempts or generate alerts, and ended on January 24, 2018 when the Entity updated their processes to require the changing of passwords and limited unsuccessful authentication attempts as well as established required alerting. Specifically, for Part 5.6, the Entity failed to enforce password changes or an obligation to change the password at least once every 15 calendar months for all eight (8) shared accounts as required by CIP-007-6 R5, Part 5.6. For Part 5.7, the Entity failed to implement controls to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts on the three (3) firewalls and four (4) switches as required by CIP-007-6 R5, Part 5.7. The root cause was an absence of internal controls related to password changes on shared accounts.
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. Specifically, the Entity's failure to change the passwords by the required timeframe could expose the passwords to malicious individuals allowing unauthorized access to Cyber Assets. This risk was increased because some of the Cyber Assets at issue were designed to provide perimeter protection to other BES Cyber Assets. Additionally, the Entity's failure to configure an account lockout policy or alerting after a certain number of failed authentication attempts, which serves to prevent unauthorized access through an online guessing or brute force attack, could have caused reliability concerns for the Entity. From July 1, 2016 to June 1, 2018 there was no known unauthorized access or breaches to any of the Entity's Cyber Assets. No harm is known to have occurred.
Mitigation	To mitigate this violation, the Entity: P5.6: 1) scheduled the process of changing the passwords for shared accounts to take place each year during the first quarter to ensure they are changed within the required timeframe; 2) set up Help Desk ticketing system that will issue auto-generated tickets the first month of each year with the list of shared accounts in the body of the ticket that need to have their passwords changed; 3) reviewed all shared accounts to ensure that all accounts are justified and still needed; 4) changed all shared account passwords; 5) configured [redacted] to monitor all shared accounts and track when passwords have been changed; and 6) generated an annual report that identifies shared accounts where the passwords have not been changed in the last 365 days. P5.7: 1) updated SIEM to analyze the logs from the firewalls and switches; 2) tested and verified logs for all applicable Cyber Assets in SIEM; 3) created rules and reporting in SIEM to produce alerts based on the threshold of 5 unsuccessful attempts occurring; and 4) trained Entity personnel on newly instituted internal controls for the requirement.

[redacted] – [redacted] NOC-2607 $0

Other Factors	FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty. FRCC reviewed the Entity's compliance history and determined there were no relevant instances of noncompliance.

[redacted] NOC-2614 $0

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
SPP2017018137	CIP-008-3	R1	Lower	High	3/17/2016 (fifteen months [redacted] had transitioned to CIP Version 5] after successful completion of the last test)	9/26/2017 (test was successfully completed)	Self-Report	8/22/2018	1/11/2019

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 August 10, 2017, [redacted] submitted a Self-Report, stating that, as a [redacted], it was in noncompliance with CIP-008-3 R1. [redacted] stated that it failed to perform an adequate test of its Cyber Security Incident response plan between December 17, 2014 and September 26, 2017. [redacted] reports that it did perform a test on March 28, 2017, but that test did not meet [redacted] standards; specifically the test was more general than [redacted] expected and did not include specific steps for implementing a response to a Cyber Security Incident to the degree that [redacted] expected. [redacted] states that it detected this noncompliance after a new CIP Senior Manager was designated and the CIP Senior Manager conducted a full review of [redacted] compliance activities. The noncompliance was caused by inadequate internal controls to provide oversight regarding the completion of this task.
Risk Assessment	The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. [redacted] conducted a test that did not meet all the requirements of its program (albeit 11 days late), thus the risk of the noncompliance was reduced because the noncompliance was essentially for conducting an incomplete test, as opposed to not conducting any type of testing. Additionally, the subsequent testing of the Cyber Security Incident plan was successful. Finally, employees are trained under CIP-004-6 R2, which includes response and recovery to Cyber Security Incidents. No harm is known to have occurred.
Mitigation	To mitigate this noncompliance, [redacted] 1) performed the required test; 2) reviewed and revised the Cyber Security Incident response plan to better align with its standards for level of detail; and 3) scheduled the next required execution of the Cyber Security Incident response plan to occur within 11 months of the last test.
Other Factors	MRO reviewed [redacted] internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. MRO considered [redacted] compliance history in determining the disposition track. [redacted] relevant prior noncompliance with CIP-008-3 R1 includes a prior moderate risk violation of CIP-008-3 R1 ([redacted] that was mitigated on [redacted]. [redacted]. In the prior violation, [redacted] conducted tests in 2012 and 2013 that were incomplete under its procedure. [redacted]. MRO considered [redacted] CIP-008-3 R1 compliance history to be an aggravating factor in the disposition track. In determining the penalty, MRO considered the investments that [redacted] has made in its compliance program since the [redacted]. At the time of the [redacted], [redacted] Finally, the noncompliance was detected after [redacted] named a new CIP Senior Manager, who undertook a review of [redacted] CIP program that included two internal audits conducted by third-party compliance companies.