

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														

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.)			<p>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.</p> <p>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.</p> <p>Specifically, the facility in scope [REDACTED] [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.</p> <p>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].</p>						
Risk Assessment			<p>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.</p> <p>The entity reduced the risk of its system becoming compromised by [REDACTED] [REDACTED]. The Low Impact system is further protected from unauthorized physical access. [REDACTED].</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">contracted third-party company to create compliance program; anddeveloped and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1. <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none">implemented automated system/tasks to ensure NERC activities are tracked and completed.						
Other Factors			<p>NPCC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p> <p>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.</p>						

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.)			<p>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.</p> <p>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.</p> <p>Specifically, the facility in scope [REDACTED] [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.</p> <p>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].</p>						
Risk Assessment			<p>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.</p> <p>The entity reduced the risk of its system becoming compromised by [REDACTED] [REDACTED]. The Low Impact system is further protected from unauthorized physical access. [REDACTED].</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">contracted third-party company to create compliance program;developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1;designated a CIP Senior Manager; andreviewed and obtained CIP Senior Manager Approval of the identified impact level. <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none">implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed						
Other Factors			<p>NPCC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p> <p>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.</p>						

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.)			<p>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.</p> <p>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.</p> <p>Specifically, the facility in scope [REDACTED] [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.</p> <p>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].</p>						
Risk Assessment			<p>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.</p> <p>The entity reduced the risk of its system becoming compromised by [REDACTED] [REDACTED]. The Low Impact system is further protected from unauthorized physical access. [REDACTED].</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">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; and5. created a facility specific CIP-003-6 procedure. <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none">1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed.						
Other Factors			<p>NPCC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p> <p>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.</p>						

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.)			<p>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.</p> <p>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. .</p> <p>Specifically, the facility in scope [REDACTED] [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.</p> <p>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].</p>						
Risk Assessment			<p>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.</p> <p>The entity reduced the risk of its system becoming compromised by [REDACTED] [REDACTED]. The Low Impact system is further protected from unauthorized physical access. [REDACTED].</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">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; and5. Created a facility specific CIP-003-6 procedure. <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none">1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed						
Other Factors			<p>NPCC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p> <p>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.</p>						

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.)			<p>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.</p> <p>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.</p> <p>Specifically, the facility in scope [REDACTED] [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.</p> <p>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].</p>						
Risk Assessment			<p>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.</p> <p>The entity reduced the risk of its system becoming compromised by [REDACTED] [REDACTED]. The Low Impact system is further protected from unauthorized physical access. [REDACTED].</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">1. identified and documented by name the CIP Senior Manager;2. contracted third-party to create compliance program; and3. created a facility specific CIP-003-6 procedure. <p>To prevent recurrence, the entity:</p> <ol style="list-style-type: none">1. implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed.						
Other Factors			<p>NPCC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>NPCC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.</p> <p>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.</p>						

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.)			<p>On July 18, 2018, the entity submitted a Self-Report stating that, as a [REDACTED], it was in violation of CIP-004-3a R3.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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.</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none"> 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			<p>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.</p> <p>[REDACTED]</p> <p>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.</p>						

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	(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.)			<p>On , WECC created a violation record for the entity, as a , 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 , to include CIP-006-3c R4. WECC created the new violation record because the increase in scope had a start date of , which was before July 1, 2016, the mandatory and enforceable date of CIP Version 5.</p> <p>Specifically, on , 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.</p> <p>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.</p> <p>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.</p> <p>This violation began on , 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 days of noncompliance.</p>						
Risk Assessment			<p>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.</p> <p>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.</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">changed the energized access key cores to the alternate access key cores at the two PSPs doors in scope;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	<p>WECC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor.</p> <p>[Redacted]</p> <p>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.</p> <p>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.</p>

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		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.)			<p>On , the entity submitted a Self-Report stating that, as , 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 . 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.</p> <p>Specifically, several issues were identified with the implementation of CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4.</p> <ul style="list-style-type: none">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 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. <p>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.</p> <p>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.</p>						

	<p>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.</p>
Risk Assessment	<p>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.</p> <p>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.</p>
Mitigation	<p>To mitigate CIP-006-6 R1 Part 1.1, the entity has:</p> <ol style="list-style-type: none">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; and4) 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. <p>To mitigate CIP-006-6 R1 Part 1.2, the entity has:</p> <ol style="list-style-type: none">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; and7) 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. <p>To mitigate CIP-006-6 R1 Part 1.3, the entity has:</p> <ol style="list-style-type: none">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; and6) audited the updated procedure for effectiveness. <p>To mitigate CIP-006-6 R1 Part 1.4, the entity has:</p> <ol style="list-style-type: none">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	<div>WECC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor.</div> <div>[Redacted]</div> <div>WECC considered the entity’s CIP-006-6 R1 compliance history and determined there were no relevant instances of noncompliance.</div>

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.)			<p>On August 14, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in violation with CIP-006-3c R1.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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]</p>						
Mitigation			<p>To remediate and mitigate this violation, the entity:</p> <ol style="list-style-type: none">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; and5) created and provided training for its updated processes and procedures to applicable personnel.						
Other Factors			<p>WECC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>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.</p> <p>The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.</p> <p>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.</p>						

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.)			<p>On June 30, 2017, the entity submitted a Self-Report stating that, as a [REDACTED], it was in violation with CIP-005-5 R2.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>However, the entity implemented strong internal controls. Specifically, the entity [REDACTED] [REDACTED] [REDACTED]. These controls lowered the likelihood of a malicious actor gaining access.</p>						
Mitigation			<p>To remediated and mitigate this violation, the entity:</p> <ul style="list-style-type: none">1) removed user access to the ESPs from the unauthorized ID;2) [REDACTED] [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; and7) implemented training of the new processes to all firewall administrators.						
Other Factors			<p>WECC reviewed the entity’s internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.</p> <p>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.</p>						

	<p>The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncompliance.</p> <p>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.</p>
--	---

			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
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.)			<p>On January 19, 2018, the entity submitted a Self-Report stating that, as a [REDACTED] it was in violation of CIP-005-5 R1.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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.</p>						
Mitigation			<p>To mitigate this violation, the entity has:</p> <ol style="list-style-type: none">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; and4) sent an email to the applicable personnel to notify them of the new peer review process.						
Other Factors			<p>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.</p> <p>The entity received mitigating credit for admitting to the violation.</p> <p>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.</p> <p>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.</p> <p>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.</p>						

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.)			<p>On February 6, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in violation of CIP-005-5 R1.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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] [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] [REDACTED]</p>						
Mitigation			<p>To mitigate this violation the entity:</p> <ol style="list-style-type: none">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; and6) held a mitigation closure meeting with applicable personnel related to all compliance elements of CIP-005-5 R1.						
Other Factors			<p>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.</p> <p>The entity received mitigating credit for admitting to the violation.</p> <p>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.</p> <p>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.</p>						

			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.						

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.)			<p>On February 3, 2017, the entity submitted a Self-Report stating, as a [REDACTED] it was in violation of CIP-007-6 R2.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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]</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none"> 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; 						

			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
			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.						

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	
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.)			<p>On February 6, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in violation of CIP-007-6 R3.</p> <p>Specifically, the entity utilized physical port locking as one of the methods to deter, detect, or prevent malicious code on its 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>							
Risk Assessment			<p>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.</p> <p>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]</p> <p>[REDACTED] This protection is provided for all devices on the network segment, including those without the anti-malware software installed. [REDACTED]</p>							
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">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; and9) 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			<p>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.</p>							

			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
			<p>The entity received mitigating credit for admitting to the violation.</p> <p>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.</p> <p>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.</p>						

			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	
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.)			<p>On February 6, 2017, the entity submitted a Self-Report stating, as a [REDACTED] it was in violation of CIP-007-6 R4.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>							
Risk Assessment			<p>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.</p> <p>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.</p>							
Mitigation			<p>To mitigate this violation the entity:</p> <ol style="list-style-type: none">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; and7) provided training to applicable personnel on the updated CIP-007-6 R4 procedures.							

			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.						

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
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.)			<p>On February 6, 2017, the entity submitted a Self-Report stating, as a [REDACTED] it was in violation of CIP-007-6 R5.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>However, the entity implemented strong controls. [REDACTED]</p> <p>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.</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">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						

			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
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 management, applicable Operations SMEs, and its Completed remediation and mitigation tasks and procedures will be discussed, reviewed, and verified.						
Other Factors			<p>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.</p> <p>The entity received mitigating credit for admitting to the violation.</p> <p>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.</p> <p>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.</p>						

			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	
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.)			<p>On [REDACTED] the entity submitted a Self-Report stating, as a [REDACTED] it was in violation of CIP-010-2 R1.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>							
Risk Assessment			<p>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.</p> <p>However, the entity implemented strong detective controls. [REDACTED]</p> <p>[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.</p>							
Mitigation			<p>To mitigate this violation, the entity has:</p> <p>1) collected the number and names of devices missing baseline elements and completed baseline configurations on the Cyber Assets in scope;</p> <p>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;</p> <p>3) upgraded applicable configuration monitoring tool device profilers to compatible firmware versions to ensure automated port scan capability;</p> <p>4) provided training to SMEs on SIEM admin, security, and compliance;</p> <p>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;</p> <p>6) promoted all 'unpromoted changes', which will set the as-is device state to be the current baseline;</p> <p>7) updated baseline reports to include only the required information to help SMEs more easily see if/when information is missing;</p>							

			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
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.						

			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
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.)			<p>On February 3, 2017, the entity submitted a Self-Report stating, as a [REDACTED], it was in violation of CIP-010-2 R2.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>						
Risk Assessment			<p>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.</p> <p>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.</p>						
Mitigation			<p>To mitigate this violation, the entity:</p> <ol style="list-style-type: none">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; and9) provided training to applicable personnel on the updated procedure.						
Other Factors			<p>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.</p> <p>The entity received mitigating credit for admitting to the violation.</p> <p>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.</p> <p>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.</p>						

			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.						