NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

January 14, 2020

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: Errata to NERC Spreadsheet Notice of Penalty regarding an Unidentified Registered Entity
FERC Docket No. NP20-6-000

Dear Ms. Bose:

On December 30, 2019, the North American Electric Reliability Corporation ("NERC") submitted the above captioned Spreadsheet Notice of Penalty regarding an Unidentified Registered Entity. NERC's filing inadvertently included a Region violation ID number.

- Accession Number: 20191230-5277 (containing A-2 Public CIP Violations), 20191230-5278 (containing A-3 Non-Public CIP Violations) FERC Docket No. NP20-6-000 filed December 30, 2019

In accordance with the Commission's Regulations, 18 C.F.R. § 388.113, NERC is providing a redacted public version of the filing. The attached files contain the pages specific to the single case in the Spreadsheet Notice of Penalty, without the Region violation ID number.

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation

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
WECC2017017507	CIP-005-5	R1: P1.1	Medium	Severe	07/01/2016	07/25/2017	Self-Report	12/04/2018	02/22/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On April 28, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-005-5 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA and submitted four additional Self-Reports. After reviewing all relevant information, WECC determined the entity failed to place the BCA connected to a network via a routable protocol, within a defined ESP as required by CIP-005-5 R1 Part 1.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on July 25, 2017, when the BCA was added to the ESP, for a total of 390 days of noncompliance. The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA.
Risk Assessment	WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and PACS [redacted]scribed here[redacted] Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets. However, as compensation, the entity had implemented managed policy rules for monitoring the BCA, and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]
Mitigation	To mitigate this violation, the entity has: 1) placed the BCA inside the ESP; and 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017631	CIP-007-6	R1: P1.1	Medium	High	07/01/2016	05/17/2017	Self-Report	09/07/2017	10/08/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA. After reviewing all relevant information, WECC determined the entity failed to enable only logical network accessible ports on the BCA that have been determined to be needed by the entity as required by CIP-007-6 R1 Part 1.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 17, 2017, when the BCA's open logical ports were documented in a baseline configuration, for a total of 321 days of noncompliance. The root cause of the violation was attributed to a lack of knowledge of the capabilities and functions of the BCA.
Risk Assessment	WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to [redacted] EACMS and [redacted] PACS as described herein. Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets. However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity has: 1) documented all enabled logical network accessible ports; and 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017632	CIP-007-6	R2: P2.1	Medium	Moderate	07/01/2016	05/09/2017	Self-Report	08/24/2018	10/23/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R2. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA. After reviewing all relevant information, WECC determined the entity failed to identify a source or sources that the entity tracks for the release of cyber security firmware patches applicable to the BCA, as required by CIP-007-6 R2 Part 2.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 9, 2017, when the BCA was added to the patch source tracking spreadsheet, for a total of 313 days of noncompliance. The root cause of this violation was attributed to a lack of knowledge of the capabilities and functions of the BCA.
Risk Assessment	WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to [redacted] EACMS and [redacted] PACS as described herein. Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets. However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity has: 1) added the BCA to the patch source tracking spreadsheet; 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and 3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected to the operations network or deployed into an ESP to include adding Cyber Assets to the patch tracking spreadsheet and documenting baseline configurations.
Other Factors	ECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues.

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
WECC2017017633	CIP-007-6	R5: P5.1-P5.7	Medium	Severe	07/01/2016	02/15/2019	Self-Report	02/15/2019	TBD

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-007-6 R5. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA. After reviewing all relevant information, WECC determined the entity failed to have method(s) to enforce authentication of interactive user access, identify and inventory all known enabled default or other generic account types, identify individuals who have authorized access to shared accounts, change known default passwords, enforce the required password length and complexity, enforce password changes at least once every 15 calendar months; and limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts where technically feasible on the BCA, as required by CIP-007-6 R5 Parts 5.1 through 5.7. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on February 15, 2019, when the protective measures as required by CIP-007-6 R5 Parts 5.1 through 5.6 were implemented and for Part 5.7 when the entity submitted a Technical Feasibility Exception, for a total of 960 days of noncompliance. The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA.
Risk Assessment	WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and [redacted]ACS as descri[redacted]erein. Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a primary [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets. However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources for [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted]. No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity has: 1) enforced authentication of interactive user access by changing the default passwords; 2) identified and inventoried all default accounts; 3) added new passwords to password safe and only allowed access to technicians with authorization to shared accounts in the password safe; 4) changed the default passwords for all accounts; 5) procedurally enforced password requirements; 6) tracked password changes in account database to be changed at least every 15 calendar months; 7) submitted to WECC a Technical Feasibility Exception for the Cyber Assets in scope not capable of limiting the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts; 8) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and 9) implemented a bi-weekly or monthly CIP collaboration meeting between technical personnel, the CIP subject matter experts, the [redacted] management to discuss such details as review of default accounts, passwords, account access logging, and asset name/role tags during the annual cyber vulnerability assessments.

Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC determined that the entity’s compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2011 and one in 2014 that posed minimal risk and are not indicative of a broader issue.

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
WECC2017017634	CIP-010-2	R1: P1.1; P1.2; P1.3	Medium	Moderate	07/01/2016	05/18/2017	Self-Report	11/16/2018	08/13/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a [redacted], it was in potential noncompliance with CIP-010-2 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one [redacted] within the Electronic Security Perimeter (ESP), used as the [redacted], and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA. The Self-Report submitted for CIP-010-2 R1 also included noncompliance related to three EACMS that did not have logical port information in the baseline configuration as required by Part 1.1 sub-part 1.1.4; for [redacted] EACMS and [redacted] PACS, the entity failed to authorize and document changes that deviated from the existing baseline configuration as required by Part 1.2; and for [redacted] EACMS and the same [redacted] PACS, made changes that deviated from the existing baseline configuration without updating the baseline configuration within 30 calendar days from completing the change as required by Part 1.3. After reviewing all relevant information, WECC determined the entity failed to develop baseline configurations for the BCA firmware and a port as required by CIP-010-2 R1 Part 1.1 sub-parts 1.1.1 and 1.1.4; develop a baseline configuration for [redacted] EACMS that included any logical network accessible ports as required by CIP-010-2 R1 Part 1.4 sub-part 1.1.4; authorize and document changes that deviated from the existing baseline configuration for [redacted] EACMS and [redacted] PACS as required by Part 1.2; and update the baseline configuration for [redacted] EACMS and [redacted] PACS as necessary within 30 calendar days of completing a change that deviated from the existing baseline configuration as required by CIP-010-2 R1 Part 1.3. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 18, 2017, when a port scan was completed, and the BCAs baseline configuration was updated, for a total of 322 days of noncompliance. The CIP-010-2 R1 instances related to the EACMS and PACS ended on June 7, 2017, when baseline configurations were authorized and updated, for a total of 342 days of noncompliance. The root cause of the BCA violations was attributed to a lack of knowledge of the capabilities and functions of the BCA. The root cause of the violations related to the EACMS and PACS was attributed to less than adequate training and miscommunications. Specifically, steps were overlooked or not performed correctly because they were being performed infrequently.
Risk Assessment	WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to two EACMS and three PACS as described herein. Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a [redacted] which could affect [redacted] at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets. However, as compensation, the entity had implemented managed policy rules for monitoring the BCA and it was in a network segment that limited permissions to communicate with other parts of the entity's network, preventing the BCA from being accessed from other network segments unless a specific rule was created to allow that communication path. To control physical access, it was located within a PSP. The BCA was used as a [redacted], but there were two backup sources [redacted]. If the primary [redacted] (the BCA) were to fail, the system would automatically switch to one of the backup sources within 30 seconds. If [redacted], the System Operator would have received an alarm and could have utilized his capability to quickly switch the [redacted] to one of the backup devices, in the event they needed to manually bypass the BCA. Additionally, the entity implemented periodic internal audits which is how the instances with the EACMS and PACS were discovered. [redacted] No harm is known to have occurred.
Mitigation	To mitigate this violation, the entity has: 1) updated and authorized baseline configurations on the Cyber Assets in scope of these violations; 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices;

	3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected to the operations network or deployed into an ESP to include documenting baseline configurations; and 4) updated the change management software to require: a. a documented baseline configuration be completed as part of the commissioning process before deploying into an ESP; and b. employees to update the baseline configuration on Cyber Assets before they can close the request for change.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC considered the entity’s compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017018364	CIP-006-6	R1: P1.5	Medium	Severe	07/01/2016	[redacted]	Compliance Audit	11/6/2018	08/19/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	During a Compliance Audit conducted [redacted], WECC determined the entity, as a [redacted], had a potential noncompliance with CIP-006-6 R1 Parts 1.4 and 1.5. Specifically, for three PSPs controlling access to MIBCSs, the entity was unable to demonstrate that it was monitoring for unauthorized access through a physical access point into each PSP as required by CIP-006-6 R1 Part 1.4, and alarms or alerts in response to detected unauthorized access through a physical access point into each PSP were issued to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection as required by CIP-006-6 R1 Part 1.5. The root cause of the violation was attributed to a misinterpretation of the Requirement Parts. Specifically, the entity believed if the PSPs were manned, no monitoring or automated alarming or alerting was needed, as such, the entity suppressed the alarms during business hours. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable, and ended on [redacted] when the entity turned on the forced entry and door held open alarms during business hours, for a total of [redacted] days of noncompliance.
Risk Assessment	WECC determined 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 monitor for unauthorized access through a physical access point into three PSPs and issue an alarm or alert in response to detected unauthorized access through a physical access point into said PSPs to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection, as required by CIP-006-6 R1 Parts 1.4 and 1.5. Such failure could potentially result in an attacker gaining access to critical systems without the entity's knowledge, prolonging the time the attacker could use for nefarious purposes and possibly allow them to escape undetected. An attacker could also monitor, manipulate, or disable Cyber Assets without entity knowledge. However, as compensation the PSPs were manned [redacted] and one of the PSPs was equipped with a camera to observe the interior of the room. [redacted]
Mitigation	To mitigate this violation, the entity has: 1) activated alarms for existing forced entry and door held open alarms during business hours; 2) updated its technician procedure for testing physical security mechanisms to include language from the Standard as a reminder of the requirements for compliance which includes verifying that door forced open and held open alarms are always communicated to the System Operators; and 3) provided training to its technical personnel on what is required for compliance with CIP-006-6 R1 and the updated procedure.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017911	CIP-007-6	R2: P2.3	Medium	Severe	10/01/2016	05/09/2017	Self-Report	09/21/2018	10/08/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On July 7, 2017, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted] Specifically, on August 26, 2016, the entity evaluated a security patch as applicable to [redacted] EACMS which it planned to install by September 30, 2016. Due to installation issues during the entity's conversion of its network from switching to routing, it was unable to install the security patch on the EACMS without interrupting service to its distribution Supervisory Control and Data Acquisition system. However, the entity did not create a dated mitigation plan within 35 calendar days of the evaluation completion as required by Part 2.3. On May 9, 2017, the entity was able to install the security patch without incident, for a total of 221 days of noncompliance. The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure which required the software to be installed on different hardware delaying the evaluation of security patches for applicability.
Risk Assessment	WECC determined 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 create a dated mitigation plan within 35 calendar days of the evaluation completion for one security patch identified as applicable to [redacted] EACMS and failed to apply one applicable security patch to [redacted] BCAs within 35 calendars days of the evaluation completion, as required by CIP-007-6 R2 Part 2.3. Such failures could have prolonged the presence of software vulnerabilities, which if exploited, could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. . However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted]
Mitigation	To mitigate this violation, the entity has: 1) evaluated security patches released since the previous evaluation; 2) installed the applicable security patch. 3) provided additional training to technical staff on security patching activities; 4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up; 5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed; 6) trained technicians on the new process; 7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program; 8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination; 9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and 10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control.
Other Factors	WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues.

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
WECC2018018977	CIP-007-6	R2: P2.3	Medium	Severe	09/29/2017	01/02/2018	Self-Report	10/05/2018	10/10/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On January 12, 2018, the entity submitted a Self-Report stating, as a [redacted] it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted] Specifically, for the first instance, on August 24, 2017, the entity evaluated a security patch as applicable to [redacted] EACMS which it planned to install by September 28, 2017. However, [redacted] and performing cyber vulnerability assessments, the installation of the security patch was overlooked, and no timely action was taken as required by Part 2.3. The security patch was installed on [redacted] of the EACMS on December 20, 2017, and a mitigation plan was created for the [redacted] remaining EACMS on December 21, 2017, for a duration of 84 days of noncompliance. For the second instance, on August 16, 2017, the entity evaluated a security patch as applicable to [redacted] BCAs which was outside of the 35 calendar day window from the previous evaluation which occurred on June 24, 2017, and again, [redacted], the entity was delayed in applying the security patch and went beyond the 35 calendar days since the evaluation completion, as required by Part 2.3. However, the entity applied the security patch on January 2, 2018, for a total of 96 days of noncompliance. The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure, which required the software to be installed on different hardware delaying the evaluation of security patches for applicability.
Risk Assessment	WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity failed to create a dated mitigation plan within 35 calendar days of the evaluation completion for one security patch identified as applicable to [redacted] EACMS and failed to apply one applicable security patch to [redacted] BCAs within 35 calendars days of the evaluation completion, as required by CIP-007-6 R2 Part 2.3. Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. . However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted]
Mitigation	To mitigate this violation, the entity has: 1) evaluated security patches released since the previous evaluation; 2) installed the applicable security patch. 3) provided additional training to technical staff on security patching activities; 4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up; 5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed; 6) trained technicians on the new process; 7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program; 8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination; 9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and 10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history was an issue in 2014 that posed minimal risk and not indicative of broader compliance issues.

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
WECC2018019483	CIP-007-6	R2: P2.2	Medium	Lower	01/31/2018	02/01/2018	Self-Report	05/21/2019	10/09/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	On April 5, 2018, the entity submitted a Self-Report stating that as a [redacted], it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located [redacted] Specifically, on December 26, 2017, the entity evaluated security patches for [redacted] PACS. The next evaluation did not occur until February 1, 2018, which was beyond the requirement to evaluate at least once every 35 calendar days, per Part 2.2, which should have been January 31, 2018, for a total of two days of noncompliance. The causes of this violation were attributed to, 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2) less than adequate patch management procedure in that it was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the stated date, and 3) software being used to track patches experiencing a server hardware failure which required the software to be installed on different hardware delaying the evaluation of security patches for applicability, respectively.
Risk Assessment	WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these instances, the entity failed to at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 for [redacted] PACS , as required by CIP-007-6 R2 Part 2.2. Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misuse of Cyber Assets that impact the reliability of the BPS. If an attacker gained access to a PACS, they could deny PSP access to authorized personnel or allow entry to unauthorized persons. The PSP controlled access to the MIBCS that if compromised could allow an attacker to manipulate, disable, or destroy Cyber Assets critical to the BPS. However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physical access. The entity did not implement controls to prevent or detect these violations. [redacted]
Mitigation	To mitigate this violation, the entity has: 1) evaluated security patches released since the previous evaluation; 2) installed the applicable security patch. 3) provided additional training to technical staff on security patching activities; 4) implemented an internal control to daily back-up the server and provide an alert to technical staff with the status of the back-up; 5) updated its patch management program to clearly define the process for creating a mitigation plan when a security patch cannot be installed; 6) trained technicians on the new process; 7) created an annual task to review the patch management program with technicians to reinforce the entire patch management program; 8) updated its patch management program with language stating that upon determination of the applicability of a patch, a change request shall be created that same day with a due date one calendar month from the day of applicability determination; 9) changed the email task reminders from being sent to just the technicians but also to management staff and the [redacted], who will escalate past-due tasks to supervisors and follow-up to ensure the task is completed; and 10) implemented emailing reports of due or past due change request tickets to assignees and management as an additional control.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2014 that posed minimal risk and not indicative of broader compliance issues.

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
WECC2017018365	CIP-007-6	R4: P4.2; Sub-part 4.2.2	Medium	High	07/01/2016	[redacted]	Compliance Audit	11/07/2018	10/09/2019

Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)	During a Compliance Audit conducted [redacted], WECC determined the entity, as a [redacted], was in potential noncompliance with CIP-007-6 R4 Part 4.2 sub-part 4.2.2. Specifically, the entity failed to generate alerts for the detected failure of event logging on [redacted] BCAs, [redacted] EACMS, and [redacted] PACS associated with the MIBCS located at [redacted] After reviewing all relevant information, WECC Enforcement concurs with the audit finding as stated above. The root cause was attributed to a design failure in that one of the rule building blocks designed to weed out false positives was in fact suppressing alerts for failed logins not associated with two-factor authentication. This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on August 29, 2017, when logging of detected failures was enabled on six of the Cyber Assets, and one Cyber Asset was decommissioned, for a total of 425 days of noncompliance.
Risk Assessment	WECC determined 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 generate alerts for security events that included detected failure of event logging for [redacted] BCAs, [redacted] EACMS, and [redacted] PACS associated with the MIBCS located at [redacted] as required by CIP-007-6 R4 Part 4.1 sub-part 4.2.2. The entity did not implement controls to detect or prevent this violation. However, as compensation the entity was able to collect logs locally even though alerting was not enabled. Additionally, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. The PACS resided within an ESP and PSP with restricted electronic and physical access. [redacted]
Mitigation	To remediate and mitigate this violation, the entity has: 1) updated the Windows auditing configuration and the SIEM alert rule which enabled alerting for detected failure of event logging for [redacted] Cyber Assets, and decommissioned one Cyber Asset; 2) updated its technician procedure to include more detail on configuring the Windows auditing section; and 3) completed initial and annual testing to ensure the SIEM is receiving and alerting on login attempts for the Cyber Assets in scope.
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC2018018977, WECC2018019483, and WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the disposition treatment to an Expedited Settlement Agreement with a $0 penalty. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant history consisted of an issue in 2014 that posed minimal risk and not indicative of broader compliance issues.