COVER PAGE

This filing 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 Notices of Penalty in this filing and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	WECC2017017388	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
2	WECC2017017390	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years

Filing Date: May 28, 2020

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
WECC2017017388	CIP-014-2	R5: P5.1	High	Lower	6/27/2016 (when the requirement was enforceable)	1/21/2020 (Mitigation Plan completion)	Compliance Audit	1/21/2020	1/29/2020

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 that the entity, as [redacted] was in violation of CIP-014-2 R5 Part 5.1. The entity did not develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities that the entity had identified during its evaluation conducted pursuant to CIP-014-2 R4. Specifically, the entity's physical security plans lacked specific mitigating measures for many of the threats identified in its R4 threat & vulnerability evaluation. At [redacted] critical facility, an identified top threat was not listed in the physical security plan with a corresponding measure of protection against said threat. Additionally, some recommended mitigating measures could not clearly be linked to which critical BES assets within a critical facility would be protected, or the identified threat that would be countered.

WECC Enforcement concurred with the audit findings as described above. The root cause of this violation was a less than adequate understanding of how to document mitigating activities to specifically address identified vulnerabilities and threats pursuant to CIP-014-2 R5 Part 5.1. This violation began on June 27, 2016, when the entity was required to implement CIP-014-2 R5 and ended on January 21, 2020 when the entity completed mitigating activities, for a total of 1,304 days of noncompliance.

Risk Assessment

This violation posed a moderate risk and did not pose a serious and substantial risk to the Bulk Power System. In this instance, the entity failed to appropriately develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted pursuant to CIP-014-2 R4. Failure to effectively counter identified critical facility and Critical Asset threats increased the risk of an unauthorized individual degrading or destroying a facility and/or Cyber Assets vital to the reliability of the BES. As CIP-014 critical facilities, these facilities are deemed necessary to the continuity of the entity's grid operations.

However, the likelihood of the risk occurring was reduced by the controls the entity had implemented. Specifically, the entity utilized [redacted] as a physical barrier at its CIP-014-2 identified facilities; had signage that provides warning information relating to video monitoring, trespassing, and safety; had multi-factor authentication access control to restrict access that alarms on detection at the perimeters; had camera surveillance strategically placed [redacted] had 24 hours-a-day, 7 days-a-week alarm monitoring and rapid response; coordinates and collaborates with law enforcement for responding to issues; [redacted] The perimeter detection provides awareness of intrusion [redacted] and [redacted] provide layered defense and alarm notification.

Additionally, the entity had [redacted] that it could use in conjunction with similar efforts [redacted] to mitigate threats to the BES. This [redacted] specifically included all Transmission stations and substations, as well as the control center identified as a part of CIP-014-2. The purpose of the plan was to use the results of a completed technical study and implement resiliency measures for each of these facilities [redacted] These additional controls helped to lessen the risk.

Mitigation

To mitigate this violation, the entity has:

1) revised its primary Control Center (PCC) threat and vulnerability assessment (TVA) documents as follows:
   a) identified and described each physical boundary and security controls deployed at each layer. The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential TVAs as constructed;
   b) ensured the [redacted] assessment (PCC only) provides a clear and appropriate view of critical components that facilitate the function of the facility and most likely vulnerabilities based on present security system capabilities. Ensured each credible TVA maps directly to solutions defined in R5 and provided a more granular approach to site protection;
   c) investigated the inclusion of an Adversary Sequence Diagram within its documentation; and

	d) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope. 2) revised its PCC physical security plans documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate those attacks to the PCC in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks; c) removed the language that identified that existing security measures at the PCC were sufficient for compliance with R5; d) reviewed and documented site deficiencies and included additional information on purpose and benefits of security measures to enhance deficiencies; and e) improved its security enhancement timeline by including security measure efficacy testing as part of implementation timeline; 3) revised substation(s) TVA documents to address items as follows: a) increased history of attacks analysis to incorporate more data on a national level to increase scope of TVA likelihood evaluation; b) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope; and c) removed the justification (Critical Components Analysis) for the differentiation of critical and non-critical components at a substation, i.e., do not apply the R1 criteria to exclude specific components from the scope of R4 and R5; 4) revised substation(s) physical security plan documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate or decrease the impact of physical attacks to substations and in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks. c) identified and described each security controls deployed at each defensible layer of the substation(s). The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential threats and vulnerabilities as constructed. Each security control will address its security measure (i.e. deter, detect, delay, communicate, assess, respond) as well as the threat the equipment is attempting to provide its security measure for. Additional emphasis and details should be included within the documentation to describe the work the entity is committing to and using at the critical sites; d) ensured all substation(s) assets that comprise a critical facility are considered, in preventing and responding to potential physical attacks. Determined that additional security measures may be required to meet site or asset protection needs. Those deemed necessary for a comprehensive physical security solution should be considered for effectiveness to overall facility operation; e) reviewed and documented site deficiencies and included additional information on the purpose and benefits of security measures to enhance deficiencies; and f) improved its security enhancement timeline by including security measure efficacy testing as part of the implementation timeline; 5) began facilitation of interdepartmental meetings that includes [redacted] in order to provide further insight on the criticality of the equipment being protected at each defined critical site; 6) began facilitation of monthly meetings of [redacted] which includes Director-level leadership of BES Cyber Systems and CIP-014-2 leadership; 7) created communication avenues for CIP topics, to include CIP-014-2 Physical Security Plans; 8) created a new position [redacted] to assist in addressing the leadership items identified within CIP-014-2. With this new position, the following benefits are derived: a) Physical and Cyber Security report [redacted] as each department plays a role in the protecting the BES; b) [redacted] is responsible for the proper execution of the NERC CIP program where in the previous organizational structure CIP-014-2 ownership was an outlier within CIP program. [redacted] meets with [redacted] every two weeks to discuss physical and cyber security issues 9) Improving CIP-014-2 knowledge from WECC as follows: a) [redacted] attended the WECC Compliance Workshop in March 2017 in San Diego, California. [redacted] b) [redacted] personnel attended monthly WECC Compliance Open Mics, and the Fall 2017 and Spring and Fall 2018 WECC Reliability and Security Workshops; c) [redacted] attended [redacted]

	10) Improving CIP-014 Knowledge from Industry perspective as follows: a) Conducted immediate outreach to CIP specialists at [redacted] and the WECC Physical Security Working Group; b) [redacted] maintained regular attendance at WECC Physical Security Working Group meetings; c) Monthly meetings with CIP subject matter experts of [redacted] and 11) Partnered with the local Police Department and Fire and Rescue for conduction of an Active Shooter Exercise [redacted] The exercise was a full-scale exercise including voluntary participation from the its employees.
Other Factors	WECC confirmed the entity did not effectively complete its mitigation of the violation; therefore, rejected the Certification of Mitigation Completion, requiring the entity to expand its mitigation and resubmit. As such, WECC escalated this moderate risk violation from an FFT to a $0 Spreadsheet Notice of Penalty. WECC determined there was no relevant compliance history.

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
WECC2017017390	CIP-014-2	R5: P5.1	High	Lower	6/27/2016 (when the requirement was enforceable)	1/21/2020 (Mitigation Plan completion)	Compliance Audit	1/21/2020	1/29/2020

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 that the entity, as [redacted] was in violation of CIP-014-2 R5 Part 5.1 The entity did not develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities that the entity had identified during its evaluation conducted pursuant to CIP-014-2 R4. Specifically, the entity's physical security plans lacked specific mitigating measures for many of the threats identified in its R4 threat & vulnerability evaluation. At [redacted] critical facility, an identified top threat was not listed in the physical security plan with a corresponding measure of protection against said threat. Additionally, some recommended mitigating measures could not clearly be linked to which critical BES assets within a critical facility would be protected, or the identified threat that would be countered.

WECC Enforcement concurred with the audit findings as described above. The root cause of this violation was a less than adequate understanding of how to document mitigating activities to specifically address identified vulnerabilities and threats pursuant to CIP-014-2 R5 Part 5.1. This violation began on June 27, 2016, when the entity was required to implement CIP-014-2 R5 and ended on January 21, 2020 when the entity completed mitigating activities, for a total of 1,304 days of noncompliance.

Risk Assessment

This violation posed a moderate risk and did not pose a serious and substantial risk to the Bulk Power System. In this instance, the entity failed to appropriately develop physical security plans that included resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted pursuant to CIP-014-2 R4. Failure to effectively counter identified critical facility and Critical Asset threats increased the risk of an unauthorized individual degrading or destroying a facility and/or Cyber Assets vital to the reliability of the BES. As CIP-014 critical facilities, these facilities were deemed necessary to the continuity of the entity's grid operations.

However, the likelihood of the risk occurring was reduced by the controls the entity had implemented. Specifically, the entity utilized [redacted] as a physical barrier at its CIP-014-2 identified facilities; had signage that provides warning information relating to video monitoring, trespassing, and safety; had multi-factor authentication access control to restrict access that alarms on detection at the perimeters; had camera surveillance strategically placed [redacted] had 24 hours-a-day, 7 days-a-week alarm monitoring and rapid response; coordinates and collaborates with law enforcement for responding to issues; and [redacted] The perimeter detection provides awareness of intrusion [redacted] and [redacted] provide layered defense and alarm notification.

Additionally, the entity had [redacted] that it could use in conjunction with similar efforts [redacted] to mitigate threats to the BES. This [redacted] specifically included all Transmission stations and substations, as well as the control center identified as a part of CIP-014-2. The purpose of the plan was to use the results of a completed technical study and implement resiliency measures for each of these facilities [redacted] hese additional controls helped to lessen the risk.

Mitigation

To mitigate this violation, the entity has:

1) revised its primary Control Center (PCC) threat and vulnerability assessment (TVA) documents as follows:
   a) identified and described each physical boundary and security controls deployed at each layer. The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential TVAs as constructed;
   b) ensured the [redacted] assessment (PCC only) provides a clear and appropriate view of critical components that facilitate the function of the facility and most likely vulnerabilities based on present security system capabilities. Ensured each credible TVA maps directly to solutions defined in R5 and provided a more granular approach to site protection;
   c) investigated the inclusion of an Adversary Sequence Diagram within its documentation; and

	d) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope. 2) revised its PCC physical security plans documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate those attacks to the PCC in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks; c) removed the language 3 that identified that existing security measures at the PCC were sufficient for compliance with R5; d) reviewed and documented site deficiencies and included additional information on purpose and benefits of security measures to enhance deficiencies; and e) improved its security enhancement timeline by including security measure efficacy testing as part of implementation timeline; 3) revised substation(s) TVA documents to address items as follows: a) increased history of attacks analysis to incorporate more data on a national level to increase scope of TVA likelihood evaluation; b) provided more quantitative evidence for the establishment of its risk threshold. Re-evaluated all potential attacks against its risk threshold, with emphasis on providing content that only removes extreme events from assessment scope; and c) removed the justification (Critical Components Analysis) for the differentiation of critical and non-critical components at a substation, i.e., do not apply the R1 criteria to exclude specific components from the scope of R4 and R5; 4) revised substation(s) physical security plan documents as follows: a) ensured its response systems and personnel designed to detect physical attacks, respond within a timeframe suitable to mitigate or decrease the impact of physical attacks to substations and in a timely manner; b) ensured physical security plans created in R5 would effectively demonstrate the capability to deter, detect, delay, assess, communicate and respond to physical attacks. c) identified and described each security controls deployed at each defensible layer of the substation(s). The defense-in-depth description will begin at the outermost perimeter, working inward to assess potential threats and vulnerabilities as constructed. Each security control will address its security measure (i.e. deter, detect, delay, communicate, assess, respond) as well as the threat the equipment is attempting to provide its security measure for. Additional emphasis and details should be included within the documentation to describe the work the entity is committing to and using at the critical sites; d) ensured all substation(s) assets that comprise a critical facility are considered, in preventing and responding to potential physical attacks. Determined that additional security measures may be required to meet site or asset protection needs. Those deemed necessary for a comprehensive physical security solution should be considered for effectiveness to overall facility operation; e) reviewed and documented site deficiencies and included additional information on the purpose and benefits of security measures to enhance deficiencies; and f) improved its security enhancement timeline by including security measure efficacy testing as part of the implementation timeline; 5) began facilitation of interdepartmental meetings that includes [redacted] in order to provide further insight on the criticality of the equipment being protected at each defined critical site; 6) began facilitation of monthly meetings of [redacted] which includes Director-level leadership of BES Cyber Systems and CIP-014-2 leadership; 7) created communication avenues for CIP topics, to include CIP-014-2 Physical Security Plans; 8) created a new position [redacted] to assist in addressing the leadership items identified within CIP-014-2. With this new position, the following benefits are derived: a) Physical and Cyber Security report [redacted] as each department plays a role in the protecting the BES; b) [redacted] is responsible for the proper execution of the NERC CIP program where in the previous organizational structure CIP-014-2 ownership was an outlier within CIP program. [redacted] meets with [redacted] every two weeks to discuss physical and cyber security issues 9) Improving CIP-014-2 knowledge from WECC as follows: a) [redacted] attended the WECC Compliance Workshop in March 2017 in San Diego, California. [redacted] b) [redacted] attended monthly WECC Compliance Open Mics, and the Fall 2017 and Spring and Fall 2018 WECC Reliability and Security Workshops; c) [redacted] attended [redacted]

	10) Improving CIP-014 Knowledge from Industry perspective as follows: a) Conducted immediate outreach to CIP specialists at [redacted] and the WECC Physical Security Working Group; b) [redacted] maintained regular attendance at WECC Physical Security Working Group meetings; c) Monthly meetings with CIP subject matter experts of [redacted] and 11) Partnered with the local Police Department and Fire and Rescue for conduction of an Active Shooter Exercise [redacted] The exercise was a full-scale exercise including voluntary participation from the its employees.
Other Factors	WECC confirmed the entity did not effectively complete its mitigation of the violation; therefore, rejected the Certification of Mitigation Completion, requiring the entity to expand its mitigation and resubmit. As such, WECC escalated this moderate risk violation from an FFT to a $0 Spreadsheet Notice of Penalty. WECC determined there was no relevant compliance history.