

816. On January 23, 2017, [REDACTED] on behalf of [REDACTED] submitted a Self-Report to, stating that, as a [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED] [REDACTED] was in violation of CIP-010-2 R3.3. *See* Self-Report, **Attachment 39c**. On August 31, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-010-2 R3; P3.1; and P3.4.¹⁵⁴ *See* Self-Report, **Attachment 39d**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-010-2 R3; P3.1, P3.3, and P3.4.¹⁵⁵ *See* Self-Report, **Attachment 39e**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-010-2 R3; P3.1, P3.3; and P3.4.¹⁵⁶ *See* Self-Report, **Attachment 39f**. This Alleged Violation includes four instances where [REDACTED] deployed a BES Cyber System (BCS) and multiple BES Cyber Assets (BCAs) into the production environment without performing active vulnerability assessments.
817. In the first instance, [REDACTED] did not perform an active vulnerability assessment on one applicable Cyber Asset (CA) prior to deploying them into the [REDACTED] production environment. Specifically, on September 22, 2016, the [REDACTED] [REDACTED] [REDACTED] subject matter expert (SME) reviewed a network anomaly report and discovered that a BCA did not have malicious software prevention tools installed. The SME reviewed [REDACTED] work management system and discovered that on September 16, 2016, [REDACTED] deployed the BCA into the production environment without performing the active vulnerability assessment per P3.3.
818. In the second instance, during a quarterly CA list review on July 20, 2016, [REDACTED] discovered that it had not documented [REDACTED] EACMs (security information and event management CA), each protecting a [REDACTED]. As a result, [REDACTED] failed to perform and document the required vulnerability assessments prior to deploying the EACMSs in the production environment and subsequent required vulnerability assessments every 15 calendar months as required by P3.1, P3.3, and P3.4.
819. This instance affected [REDACTED]
[REDACTED] [REDACTED]

¹⁵⁴ This was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-010-2 R3 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R2 is the applicable Standard and Requirement.

¹⁵⁵ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-010-2 R3 is the applicable Standard and Requirement.

¹⁵⁶ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-010-2 R3 is the applicable Standard and Requirement.

820. In the third instance, during a CA categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] operating as EACMSs. As a result, [REDACTED] failed to perform and document the required vulnerability assessments prior to deploying the [REDACTED] in the production environment and subsequent required vulnerability assessments every 15 and 36 calendar months as required by P3.1, P3.3, and P3.4.
821. This instance affected [REDACTED].
822. In the fourth instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to perform and document the required vulnerability assessments prior to deploying the EACMS servers in the production environment and subsequent required vulnerability assessments every 15 calendar months as required by P3.1, P3.3, and P3.4.
823. This instance affected a total of [REDACTED].
824. The Alleged Violation started July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED] when [REDACTED] committed to completing its Mitigation Plan.

Aggregate Contributing Causes of CIP-010-2 R3 Alleged Violations

825. The primary cause of the CIP-010-2 R3 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. [REDACTED] configuration change management process did not clearly define the roles and responsibilities of [REDACTED] personnel, which created inconsistent application of the process. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations. Additionally, there was a lack of internal controls to ensure that specific actions required by the process were followed.

Aggregate Risk Statement for CIP-010-2 R3 Alleged Violations

826. The Regions determined that the Alleged Violation posed an aggregate moderate risk¹⁵⁷ to the reliability of the Bulk Power System.¹⁵⁸ The risk posed by [REDACTED]

¹⁵⁷ All Alleged Violations, individually, posed a moderate risk to the reliability of the BPS.

¹⁵⁸ CIP-010-2 P3.3 has a VRF of “Medium” pursuant to CIP-010-2 Table of Compliance Elements. According to the VSL Matrix, this issue warranted a “Severe” VSL.

[REDACTED]

failure to conduct vulnerability assessments of CAs prior to deploying them into the production environments was providing the opportunity of unsecured CAs which, if exploited, could lead to unauthorized changes to BCSs. Notwithstanding, the subject devices were protected inside a 24/7 monitored Physical Security Perimeter. Further, all devices, except for the issues involving asset identification in the last Alleged Violation, were protected within a secured Electronic Security Perimeter. Regarding the PCA, it was not critical to the operations of the [REDACTED] [REDACTED] and was not connected to the [REDACTED]. The duration for all Alleged Violations ranged from six to twelve days.

Mitigating Actions for CIP-010-2 R3 Alleged Violations

827. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-010-2 R3 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
828. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
829. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

LL. CIP-010-2 R4 [REDACTED]

830. CIP-010-2 prevents and detects unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

831. CIP-010-2 R4 provides:

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

Description of Alleged Violation for [REDACTED]

832. On November 11, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as [REDACTED] [REDACTED] [REDACTED] and [REDACTED] they were in violation of CIP-010-2 R4. *See* Self-Report, **Attachment 40a**. This Alleged Violation involves multiple instances where [REDACTED] failed to implement one or more documented plans for Transient Cyber Assets (TCAs).
833. On May 30, 2017, [REDACTED] discovered four instances of noncompliance. In the first instance, two IT support personnel were granted unauthorized access to [REDACTED] TCAs (Attachment 1, Section 1.2). On December 15, 2017, the [REDACTED] [REDACTED] authorized these IT support personnel as TCA users.¹⁵⁹
834. In the second instance, between May 2017 and January 16, 2018, [REDACTED] installed and uninstalled application software to [REDACTED] TCAs without prior authorization (Attachment 1, Section 1, paragraph 1.2).
835. In the third instance, one TCA had at least one missing patch in violation (Attachment 1, Section 1, paragraph 1.3.) In the fourth instance, patch tracking documentation was unavailable for [REDACTED] TCAs (Attachment 1, Section 2, paragraph 2.1).
836. [REDACTED] conducted an extent of condition and discovered additional instances of unauthorized software residing on TCAs and additional instances of missing patches. [REDACTED] did not install certain anti-virus components on TCAs. The lack of this anti-virus component [REDACTED] often used to connect a TCA to a BES Cyber Asset (BCA).
837. The Alleged Violation affected [REDACTED] BES Cyber Systems (BCSs) containing [REDACTED] Cyber Assets (CAs).
838. The Alleged Violation started on April 1, 2017, when, in the first and fourth instances, the Standard became mandatory and enforceable, and will end on [REDACTED]

¹⁵⁹ [REDACTED] [REDACTED] was unable to determine when this occurred, stating because the logs were no longer available. Therefore, [REDACTED] is using the CIP-010-2 implementation date as the start of the noncompliance.

[REDACTED], the date [REDACTED] committed to complete its Mitigation Plan.

Description of Alleged Violation for [REDACTED]

839. On November 28, 2017, [REDACTED] submitted a Self-Report stating that, as a [REDACTED] it was in violation of CIP-010-2 R4. *See* Self-Report, **Attachment 40b**. [REDACTED] did not use an approved TCA when connecting to a BCA to change passwords.
840. On July 26, 2017, two [REDACTED] personnel were at a Medium Impact BES facility to change passwords on [REDACTED]. At 1:40 p.m., one employee connected a [REDACTED] issued laptop, which was not an approved TCA to a BCA at the facility and began the process of changing [REDACTED] passwords. At 3:00 p.m., a different employee noticed the approved TCA nearby, and the employee utilizing the unapproved laptop immediately disconnected it from the BCA.
841. This Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
842. The Alleged Violation started on July 26, 2017 at 1:40 p.m., when [REDACTED] connected an unapproved laptop to a BCA, and ended on July 26, 2017 at 3:00 p.m., when [REDACTED] disconnected the unapproved laptop from the BCA.

Aggregate Contributing Causes of CIP-010-2 R4 Alleged Violations

843. The primary cause of the CIP-010-2 R4 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process and implemented stronger internal controls to help ensure that the process was sufficient and followed. However, [REDACTED] process did not clearly cover TCAs. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations. Additionally, there was a lack of internal controls to ensure that specific actions required by the process were followed.

Aggregate Risk Statement for CIP-010-2 R4 Alleged Violations

844. The Regions determined that the Alleged Violations posed an aggregate serious risk¹⁶⁰ to the reliability of the Bulk Power System based on the following factors.¹⁶¹ [REDACTED] failure to manage the implementation of TCAs led to multiple failures in managing baseline configurations, unauthorized access to TCAs, and inadequate

¹⁶⁰ Alleged Violation [REDACTED] individually posed a serious risk to the reliability of the BPS, and [REDACTED] individually, posed a minimal risk.

¹⁶¹ CIP-010-2 P1 has a VRF of “Medium” pursuant to CIP-010-2 Table of Compliance Elements. According to the VSL Matrix, these Alleged Violations warrant a “Severe” VSL.

[REDACTED]

patch management. The risk posed was providing the opportunity for manipulation of sensitive data or placing malicious software on the TCAs, which could have been used to attack CAs within ESPs. However, [REDACTED] implemented the following protective measures. The affected BCSs and their associated CAs were protected inside a 24/7 monitored Physical Security Perimeter and ESP. Regarding the Alleged Violation where the employee connected a [REDACTED] issued laptop to a BCA at change relay passwords, the duration of the noncompliance was slightly over an hour and the anti-virus software on the [REDACTED] issued corporate laptop was updated the previous day. The laptop was never re-purposed and was under the control of vetted personnel while outside the subject ESPs.

845. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. In the first Alleged Violation, [REDACTED] had four separate instances in which it either granted unauthorized access to TCAs, installed software to TCAs without authorization, missed patches on TCAs, or failed to have patch tracking documentation. The Alleged Violation affected more than [REDACTED] TCAs. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-010-2 R4 Alleged Violations

846. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-010-2 R4 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
847. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable

848. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED]. [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

████████████████████

850. CIP-011-2 R1 provides:

P.1.1. Method(s) to identify information that meets the definition of BES Cyber System Information.

P1.2. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

852. On April 19, 2017, a [REDACTED] employee was working with a vendor, via video conference, to troubleshoot an uploading error associated with a newly implemented asset database used to manage BES Cyber Assets (BCAs). The vendor could not determine the cause of the error and requested BSCI, including a copy of the production database and any files the employee was using.

[REDACTED]

so that the vendor could recreate the employee's cyber environment to troubleshoot the error. The employee transferred the requested BCSI to the vendor's support website using [REDACTED]. However, [REDACTED] is not an accepted protocol in [REDACTED] information protection program for transmitting BSCI.

853. On April 20, 2017, the employee realized the error, immediately contacted the vendor, and requested that the vendor delete all BCSI transferred the previous day. That same day the vendor confirmed with the employee that the vendor deleted the data, did not copy or back up the data, and confirmed no one else had viewed the data.
854. The BCSI that [REDACTED] sent to the vendor included information for most, if not all, servers and data center appliances managed within the [REDACTED] footprint.
855. The Alleged Violation started on April 19, 2017, when the employee sent the BCSI to the vendor, and ended on April 20, 2017, when the vendor deleted the information.

Description of Alleged Violation for [REDACTED]

856. On August 3, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation of CIP-011-2 R1; P1.2.¹⁶² See Self-Report, **Attachment 41b**. [REDACTED] failed to protect and securely handle BCSI in accordance with its information protection program.
857. On June 30, 2017, a [REDACTED] project manager [REDACTED] BCSI to a contractor without labeling the information as BCSI and without using a secure method of transmittal as prescribed in [REDACTED] information protection program. The contractor requested information about the workstations in the new control center to complete a configuration step for which the contractor was responsible. The project manager [REDACTED] containing the names of the workstations and the applied security patches, enabled ports, and IP addresses associated with the workstations, which was more information than the contractor requested. A couple of hours later, during a meeting between the project manager and contractor, the contractor advised [REDACTED] of the improper data transmittal of the BCSI.
858. The Alleged Violation affected [REDACTED] [REDACTED] [REDACTED] BCS, [REDACTED] BCAs, and [REDACTED] Protected Cyber Assets (PCAs).

¹⁶² The Alleged Violation was self-reported under P1.1 and P1.2; however, the Regions determined that P1.2 is the only applicable Requirement.

859. The Alleged Violation started and ended on June 30, 2017, when the [REDACTED] project manager employee sent unsecured BCSI [REDACTED].

Description of Alleged Violation for [REDACTED]

860. On November 6, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-011-2 R1; P1.2.¹⁶³ See Self-Report, **Attachment 41c**. [REDACTED] failed to protect and securely handle BCSI in accordance with its information protection program.
861. On June 28, 2017, while preparing to add a new repository and determining access to that repository, [REDACTED] discovered that system administrator access to [REDACTED] total repositories had not been logged. As a result, logs were unavailable for management to review and verify for accuracy and that individuals had a business need to access BCSI repositories. [REDACTED] information protection program requires the logging of individuals who electronically access BCSI repositories and periodic management review of logs to verify they are correct and that those accessing BCSI repositories have a business need to do so.
862. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and ended on December 13, 2017, when logs became available and [REDACTED] began reviewing and verifying the logs.

Description of Alleged Violation for [REDACTED]

863. On December 18, 2017, [REDACTED] submitted a Self-Report to [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-011-2 R1; P1.2. See Self-Report, **Attachment 41d**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] [REDACTED] and [REDACTED] it was in violation of CIP-011-2 R1; P1.1; P1.2. See Self-Report, **Attachment 41e**.¹⁶⁴ On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as a [REDACTED] it was in violation of CIP-011-2 R1; P1.1; P1.2. See Self-Report, **Attachment 41f**.¹⁶⁵ This Alleged Violation includes three instances where [REDACTED] failed to identify and securely protect BCSI in accordance with its

¹⁶³ The Alleged Violation was self-reported under CIP-004-6 R4.4; however, the Regions determined that CIP-011-2; R1; P1.2 is the applicable Standard and Requirement.

¹⁶⁴ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-011-2 R1 is the applicable Standard and Requirement.

¹⁶⁵ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-011-2 R1 is the applicable Standard and Requirement.

[REDACTED]

information protection program.

864. In the first instance, on October 5, 2017, [REDACTED] discovered that during the initial BCS information identification process conducted in late 2015, it did not identify a software program that managed [REDACTED] testing as a BCS information repository per [REDACTED] information protection program.
865. This instance affected [REDACTED] [REDACTED] [REDACTED] BCSs, [REDACTED] BCAs, and [REDACTED] PCAs.
866. In the second instance, during a Cyber Asset (CA) categorization review on January 5, 2017, [REDACTED] discovered that it had not identified [REDACTED] as EACMSs. As a result, [REDACTED] failed to implement the BCSI identification and protection requirements to the EACMSs in accordance with its information protection program.
867. This instance affected facilities include [REDACTED] BCSs, which consisted of [REDACTED] EACMSs.
868. In the third instance, as part of an extent of condition assessment on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as Intermediate Systems or EACMSs. As a result, [REDACTED] failed to implement the BCSI identification and protection requirements to the EACMS servers in accordance with its information protection program.
869. This instance affected a total of [REDACTED] EACMSs and [REDACTED] PACS, all associated with [REDACTED] BCSs.
870. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable, and will end on [REDACTED], when [REDACTED] committed to complete its Mitigation Plan.

Aggregate Root Cause of CIP-011-2 R1 Alleged Violations

871. The primary cause of the CIP-011-2 R1 Alleged Violations was lack of managerial oversight. Contributing causes included a deficient process, inadequate training, and lack of internal controls. Proper managerial oversight should have identified and prevented deficiencies in the process to help ensure that the process was sufficient and followed. The process did not clearly define the individual roles and responsibilities for capturing all individuals with access to BCSI repositories and did not include sufficient guidance for identifying repositories. Additionally, staff were not aware of the NERC CIP requirements for labeling and externally sending BCSI. Additional training, along with clearer instructions for completing tasks, could have helped prevent the Alleged Violations.

Aggregate Risk Assessment for CIP-011-2 R1 Alleged Violations

872. The Regions determined that the Alleged Violations posed an aggregate serious and substantial risk¹⁶⁶ to the reliability of the Bulk Power System.¹⁶⁷ The risk posed by [REDACTED] failure to identify all BCSI and securely handle it in accordance with the documented program was providing the opportunity for an individual with malicious intent to gain access to highly sensitive information, gain access to CAs and BPS facilities, and cause grid instability. However, [REDACTED] did implement the following protective measures. For the Alleged Violation where BCSI was sent to the vendor to troubleshoot an asset database uploading error, the [REDACTED] [REDACTED] In addition, a non-disclosure agreement between the vendor and [REDACTED] was in place, which required the vendor to treat all data with complete confidentiality and to properly destroy the data when troubleshooting efforts were completed. The duration of the Alleged Violation was only one day. Regarding the Alleged Violation where BSCI was sent to a contractor performing work at a control center, the contractor was actively engaged in the project and needed the BCSI to perform his duties. Additionally, the [REDACTED] and the contractor had executed a non-disclosure agreement to restrict the sharing of BCSI. Moreover, access credentials would have been required to assume control of BCAs. For the Alleged Violation where the software program was not identified as a BCSI, the software program was protected inside an ESP, protected by two-factor authentication, which required individuals with access to have completed a valid background check and cyber security training.
873. Despite these protective measures, the aggregate risk remains serious and substantial based on several factors. In addition to the multiple violations involving BCSI, for the Alleged Violation where system administrator access repositories had not been logged, the BCSI contained clear text passwords, the Alleged Violation affected all [REDACTED] of [REDACTED] functional groups, [REDACTED] did not know where all of their BSCI data resided, and the duration of the Alleged Violation was over two years. The Regions determined that [REDACTED] had serious, systemic security and compliance issues across its [REDACTED] functional groups, which required [REDACTED] to overhaul its entire CIP compliance program. Because of this, the risk for continued noncompliance and compromise to BCSs and CAs dramatically increased. Due to the weaknesses in [REDACTED] CIP compliance program, the Regions anticipate that [REDACTED] will identify

¹⁶⁶ Alleged Violations [REDACTED] individually posed a moderate risk to the reliability of the BPS, and [REDACTED] individually posed a serious.

¹⁶⁷ CIP-0011-2 R1.2 has a VRF of “Medium” pursuant to the CIP-011-2 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a “Severe” VSL.

additional instances of noncompliance while completing mitigation, which [REDACTED] will report to the Regions. Notwithstanding, [REDACTED] comprehensive mitigation should address all Alleged Violations and any additional instance(s) of noncompliance that [REDACTED] reports.

Mitigating Actions for CIP-011-2 R1

874. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-011-2 R1 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.

875. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.

876. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

NN. CIP-011-2 R2 [REDACTED]

877. CIP-011-2 prevents unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

878. CIP-011-2 R2 provides:

R2. Each Responsible Entity shall implement one or more documented

process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.

P2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

P2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

Description of Alleged Violation and Risk Assessment for [REDACTED]

879. On [REDACTED] [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-011-2 R2; P2.1; and P2.2.¹⁶⁹ See Self-Report, **Attachment 42a**. On April 7, 2017, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] stating that, as a [REDACTED] and [REDACTED] it was in violation CIP-011-2 R2; P2.1; and P2.2.¹⁷⁰ See Self-Report, **Attachment 42b**. On January 23, 2018, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] [REDACTED] [REDACTED] [REDACTED] stating that, as [REDACTED] they were in violation of CIP-011-2 R2; P2.1; and P2.2.¹⁷¹ See Self-Report, **Attachment 42c**. This Alleged Violation includes three instances where [REDACTED] failed to protect BES Cyber System Information (BCSI) in accordance with its information protection program.

880. In the first instance, during a quarterly Cyber Asset (CA) list review on [REDACTED] [REDACTED], [REDACTED] determined that it had not identified EACMSs. As a result, [REDACTED] failed

¹⁶⁸ This Alleged Violation was an audit finding under CIP-008-5 R1. However, the Regions determined that there was not a violation of CIP-008-5 R1 and is using this NERC Violation ID to process the EACMS instances.

¹⁶⁹ This was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R2 is the applicable Standard and Requirement.

¹⁷⁰ This noncompliance was self-reported under CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R1 is the applicable Standard and Requirement.

¹⁷¹ This noncompliance was self-reported as CIP-002-5.1a R1 and assigned NERC Tracking Number [REDACTED]. However, CIP-002-5.1a R1 does not apply to EACMSs; therefore, the Regions determined that CIP-007-6 R1 is the applicable Standard and Requirement.

[REDACTED]

to take action to prevent the unauthorized retrieval of BCSI from the CA data storage media.

881. This instance affected [REDACTED]
882. In the second instance, during a CA categorization review on January 5, 2017, [REDACTED] determined that it had not identified [REDACTED] as EACMSs. As a result, [REDACTED] failed to take action to prevent the unauthorized retrieval of BCSI from the CA data storage media.
883. This instance affected a total of [REDACTED] EACMSs associated with [REDACTED] BCSs.
884. In the third instance, as part of an extent of condition review on November 15, 2017, [REDACTED] determined that it had not identified [REDACTED] servers as EACMSs. As a result, [REDACTED] failed to take action to prevent the unauthorized retrieval of BCSI from the CA data storage media.
885. This instance affected a total of [REDACTED] EACMSs and [REDACTED] PACSs, all associated with [REDACTED] BCSs.
886. The primary cause of this Alleged Violation was insufficient training on identifying in-scope cyber assets. [REDACTED] training lacked the specificity to ensure that it identified EACMSs.
887. The Alleged Violation started on July 1, 2016, when the Standard became mandatory and enforceable and [REDACTED] failed to provide the protections required by CIP-011-2 R2, and will end on [REDACTED] the date [REDACTED] committed to complete its Mitigation Plan.
888. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the Bulk Power System (BPS).¹⁷² Prior to the release for reuse of these EACMS that contain BCSI, [REDACTED] failure to take action to prevent the unauthorized retrieval of BCSI from the CA data storage media for these EACMS could leave the Cyber System information on these devices vulnerable to an attack. These inactions could lead to access of sensitive data which could negatively affect BPS reliability. However, [REDACTED] deployed the devices in question behind a firewall, it logged events to detect malicious code, as well as successful and failed login attempts, and it changed known default password per CA capability and enforced password complexity. [REDACTED] also deployed methods to enforce authentication of

¹⁷²CIP-011-2 R2 has a VRF of “Lower” pursuant to the CIP-011-2 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a “Severe” VSL.

interactive user access.

Mitigating Actions for CIP-011-2 R2

889. On September 11, 2018, [REDACTED] submitted to [REDACTED] its final Mitigation Activities to address the CIP-011-2 R2 Alleged Violations. *See* Mitigation Activities, **Attachment 2e**. On September 28, 2018, [REDACTED] accepted the Mitigation Activities.
890. In the Mitigation Activities, [REDACTED] committed to take the following actions by [REDACTED] (i) revise its overarching corporate [REDACTED] program to ensure that it meets the requirements of all stakeholders and the CIP Standards; (ii) each [REDACTED] business unit will develop new and/or revise existing processes and procedures and internal controls to ensure that each business unit adheres to the [REDACTED] program; (iii) each business unit will conduct training on new and/or revised processes and procedures; (iv) each business unit will implement new and/or revised process and procedures, including documenting and tracking all internal controls for CIP compliance; and (v) [REDACTED] will document how each noncompliance identified in the Settlement Agreement was mitigated and how such mitigation will prevent recurrence via a mitigation citation document. The citation document will be organized by Standard and Requirement under CIP Version 5/6 and will reference the applicable milestones and associated mitigation activities in the consolidated Mitigation Plan. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the V3-V5 Compatibility Tables.
891. Upon completion of these Mitigation Activities, [REDACTED] shall promptly provide evidence supporting the completion to [REDACTED] [REDACTED] will verify [REDACTED] completion of the Mitigation Activities and promptly report its successful completion to NERC.

OO. CIP-014-2 R1 [REDACTED]

892. CIP-014-2 requires an entity to identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.
893. CIP-014-2 R1 provides:
- R1.** Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or

transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

Description of Alleged Violation and Risk Assessment for [REDACTED]

894. On July 11, 2016, [REDACTED] submitted a Self-Report to [REDACTED] on behalf of [REDACTED] stating that, as a [REDACTED] [REDACTED] was in violation of CIP-014-2 R1.¹⁷³ See Self-Report, **Attachment 43a**. [REDACTED] risk assessment of transmission substations did not include one applicable substation.
895. On July 21, 2015, [REDACTED] conducted a preliminary review of its substation list and removed a transmission substation because [REDACTED] determined that it was not applicable to Applicability Section 4.1.1.1 of the standard (collector bus for generation plant criteria). On September 1, 2015, [REDACTED] performed its assessment of the remaining substations, and on September 4, 2015, [REDACTED] provided its completed assessment to an unaffiliated third-party for review per CIP-014-2 R2.
896. On April 28, 2016, during a [REDACTED] staff meeting, [REDACTED] discovered that the removed substation met criteria in Applicability Section 4.1.1.2 of the standard based on the build-out that [REDACTED] would be completing in December 2016. The substation would have an “aggregate weighted value exceeding 3000” based on the number of transmission lines. On May 6, 2016, [REDACTED] [REDACTED] reviewed the assessment methodology and verified that the transmission substation met the criteria in Applicability Section 4.1.1.2 of the standard.
897. The primary cause was a misapplication of the criteria in the Applicability Section of the standard when reviewing the transmission substations list by not applying all criteria.
898. The Alleged Violation started on September 1, 2015, when [REDACTED] failed to include the transmission substation in its CIP-014-2 R1 risk assessment, and ended on June 17, 2016, when [REDACTED] completed the risk assessment reflecting the missing substation.
899. The Regions determined that the Alleged Violation posed a moderate risk to the reliability of the BPS.¹⁷⁴ [REDACTED] failure to perform an assessment of all applicable

¹⁷³ The Alleged Violation was self-reported under CIP-014-2 R2; however, the Regions determined that R1 is the applicable Standard Requirement.

¹⁷⁴ CIP-014-2 R1 has a VRF of “High” pursuant to the CIP-011-2 Table of Compliance Elements. According to the VSL Matrix, this violation warranted a “Severe” VSL.

[REDACTED]

transmission substations presented the risk that [REDACTED] would be unable to identify a substation that became inoperable or damaged as a result of an attack. The risk was mitigated because the transmission substation did not meet the criterion outlined under the standard until [REDACTED], when the substation build-out was completed, and [REDACTED] completed the risk assessment including the substation in June 2016.

Mitigating Actions for CIP-014-2 R1

900. On July 18, 2017, [REDACTED] submitted to [REDACTED] its final Mitigation Plan to address the CIP-014-2 R1 Alleged Violation. *See* [REDACTED] **Attachment 43b**. On August 18, 2017, [REDACTED] accepted the Mitigation Plan.
901. To mitigate this violation, [REDACTED] (i) ran a special assessment on the substation in question and shared results with its unaffiliated third-party vendor; (ii) revisited CIP-014 best practices with other [REDACTED] [REDACTED] corporate affiliates; and (iii) modified and republished its CIP-014-2 methodology so that in future assessments, it will include all transmission station and substations to be shared with the unaffiliated third-party verifier, making no exclusions for Applicability Section 4.1.1.
902. On August 25, 2017 [REDACTED] certified that it completed this Mitigation Plan on September 30, 2016. *See* Certification of Completed Mitigation Plan, **Attachment 43c**. [REDACTED] will verify [REDACTED] completion of the Mitigation Plan and report its successful completion to NERC

Attachment 1 – Compliance History

1. Regarding CIP-002-1 R1, [REDACTED] prior violations are as follows:
[REDACTED]
2. Regarding CIP-002-1 R2, [REDACTED] prior violations are as follows:
[REDACTED]
3. Regarding CIP-002-1 R3, [REDACTED] prior violations are as follows:
[REDACTED]
4. Regarding CIP-002-3 R3, [REDACTED] prior violations are as follows:
[REDACTED]
5. Regarding CIP-003-1 R4, [REDACTED] prior violations are as follows:
[REDACTED]
6. Regarding CIP-003-1 R5, [REDACTED] prior violations are as follows:
[REDACTED]
7. Regarding CIP-003-1 R6, [REDACTED] prior violations are as follows:
[REDACTED]
8. Regarding CIP-003-3 R1, [REDACTED] prior violations are as follows:
[REDACTED]
9. Regarding CIP-003-3 R4, [REDACTED] prior violations are as follows:
[REDACTED]
10. Regarding CIP-003-3 R5, [REDACTED] prior violations are as follows:
[REDACTED]. Regarding CIP-003-3 R6, [REDACTED] prior violations are as follows:
[REDACTED]
11. Regarding CIP-004-1 R2, [REDACTED] prior violations are as follows:
[REDACTED]
12. Regarding CIP-004-1 R3, [REDACTED] prior violations are as follows:
[REDACTED]
13. Regarding CIP-004-1 R4, [REDACTED] prior violations are as follows:
[REDACTED]
14. Regarding CIP-004-3 R2, [REDACTED] prior violations are as follows:
[REDACTED]
15. Regarding CIP-004-3 R4, [REDACTED] prior violations are as follows:
[REDACTED]
16. Regarding CIP-004-3a R2, [REDACTED] prior violations are as follows:
[REDACTED]

17. Regarding CIP-004-3a R4, [REDACTED] prior violations are as follows:
[REDACTED]

18. Regarding CIP-005-1 R1, [REDACTED] prior violations are as follows:
[REDACTED]

19. Regarding CIP-005-1 R2, [REDACTED] prior violations are as follows:
[REDACTED]

20. Regarding CIP-005-1 R3, [REDACTED] prior violations are as follows:
[REDACTED]

21. Regarding CIP-005-1 R4, [REDACTED] prior violations are as follows:
[REDACTED]

22. Regarding CIP-005-1 R5, [REDACTED] prior violations are as follows:
[REDACTED]

23. Regarding CIP-005-3 R4, [REDACTED] prior violations are as follows:
[REDACTED]

24. Regarding CIP-005-3a R1, [REDACTED] prior violations are as follows:
[REDACTED]

25. Regarding CIP-005-3a R2, [REDACTED] prior violations are as follows:
[REDACTED]

26. Regarding CIP-005-3a R3, [REDACTED] prior violations are as follows:
[REDACTED]

27. Regarding CIP-005-3a R4, [REDACTED] prior violations are as follows:
[REDACTED]

Regarding CIP-005-3a R5, [REDACTED] prior violations are as follows:
[REDACTED]

28. Regarding CIP-006-1 R1, [REDACTED] prior violations are as follows:
[REDACTED]

[REDACTED]

29. Regarding CIP-006-1 R2, [REDACTED] prior violations are as follows:
[REDACTED]

30. Regarding CIP-006-1 R3, [REDACTED] prior violations are as follows:
[REDACTED]

31. Regarding CIP-006-1 R4, [REDACTED] prior violations are as follows:
[REDACTED]

32. Regarding CIP-006-2 R5, [REDACTED] prior violations are as follows:
[REDACTED]

33. Regarding CIP-006-3a R1, [REDACTED] prior violations are as follows:
[REDACTED]

34. Regarding CIP-006-3c R1, [REDACTED] prior violations are as follows:
[REDACTED]

35. Regarding CIP-006-3c R2, [REDACTED] prior violations are as follows:
[REDACTED]

36. Regarding CIP-006-3c R4, [REDACTED] prior violations are as follows:
[REDACTED]

37. Regarding CIP-006-3c R5, [REDACTED] prior violations are as follows:
[REDACTED]

38. Regarding CIP-006-3c R6, [REDACTED] prior violations are as follows:
[REDACTED]

39. [REDACTED] Regarding CIP-006-3c R8,
[REDACTED] prior violations are as follows: [REDACTED]

40. Regarding CIP-007-1 R1, [REDACTED] prior violations are as follows:
[REDACTED]

41. Regarding CIP-007-1 R2, [REDACTED] prior violations are as follows:
[REDACTED]

42. Regarding CIP-007-1 R3, [REDACTED] prior violations are as follows:
[REDACTED]

43. Regarding CIP-007-1 R4, [REDACTED] prior violations are as follows:
[REDACTED]

44. Regarding CIP-007-1 R5, [REDACTED] prior violations are as follows:
[REDACTED]

[REDACTED]

45. Regarding CIP-007-1 R6, [REDACTED] prior violations are as follows:

[REDACTED]

46. Regarding CIP-007-1 R8, [REDACTED] prior violations are as follows:

[REDACTED]

47. Regarding CIP-007-2a R5, [REDACTED] prior violations are as follows:
[REDACTED] Regarding CIP-007-2a R6, [REDACTED] prior violations are as follows:

48. Regarding CIP-007-3a R1, [REDACTED] prior violations are as follows:

[REDACTED]

Regarding CIP-007-3a R3, [REDACTED] prior violations are as follows:

[REDACTED]

49. Regarding CIP-007-3a R4, [REDACTED] prior violations are as follows:

[REDACTED]

50. Regarding CIP-007-3a R5, [REDACTED] prior violations are as follows:

[REDACTED]

51. Regarding CIP-007-3a R6, [REDACTED] prior violations are as follows:

[REDACTED]

52. Regarding CIP-007-3a R7, [REDACTED] prior violations are as follows:

[REDACTED]

53. Regarding CIP-007-3a R8, [REDACTED] prior violations are as follows:

[REDACTED]

54. Regarding CIP-008-1 R1, [REDACTED] prior violations are as follows:

[REDACTED]

55. Regarding CIP-009-1 R5, [REDACTED] prior violations are as follows:

[REDACTED]

56. Regarding CIP-009-3 R5, [REDACTED] prior violations are as follows:

[REDACTED]

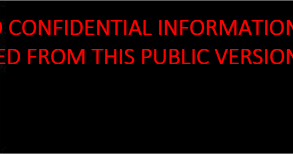
Attachment 2

The Companies' mitigation activities to address the CIP-002-5 through CIP-011-2 violations

CIP Program Area: BES Cyber System Categorization (CIP-002)

Business Unit		BES Cyber System Categorization			
	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none">Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file.	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none">[REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”¹
	[REDACTED]				

¹ Available at <https://www.nerc.com/pa/CI/Documents/V3-V5%20Compatibility%20Tables.pdf>.

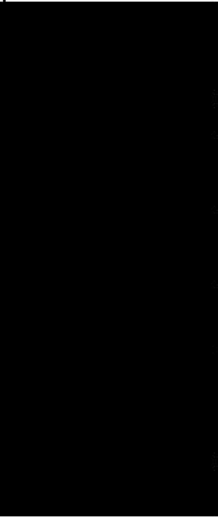





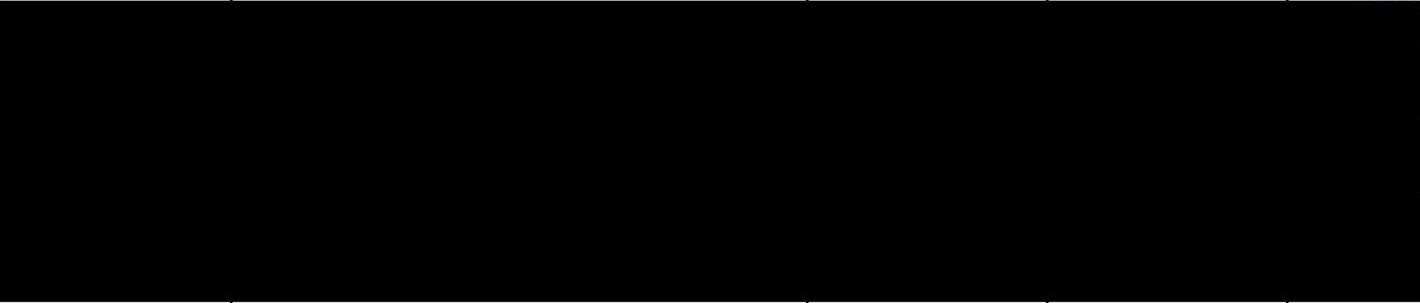


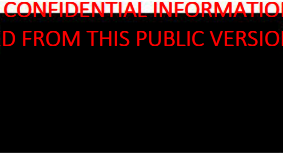
CIP Program Area: Personnel & Training (CIP-004)

Business Unit		Personnel & Training			
<div></div>	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none">Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file.	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none">[REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”
	<div></div>				



CIP Program Area: Electronic Security Perimeter(s) (CIP-005)

Business Unit		Electronic Security Perimeter(s)			
	Milestone 1: Ensure  program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the  requirements <ul style="list-style-type: none">Each  business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or  will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file.	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none"> will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”
					

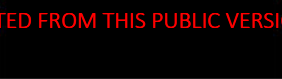


CIP Program Area: Physical Security of BES Cyber Systems (CIP-006)

Business Unit		Physical Security of BES Cyber Systems			
<div></div>	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none">Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file.	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none">[REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”

1000 JOURNAL OF CLIMATE

Business Unit		System Security Management			
	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none"> Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file. 	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none"> [REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”
[REDACTED]	[REDACTED]				
	[REDACTED]				
	[REDACTED]				
	[REDACTED]				
	[REDACTED]				



CIP Program Area: Recovery Plans for BES Cyber Systems (CIP-009)

Business Unit		Recovery Plans for BES Cyber Systems			
	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none">Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file.	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none">[REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”

REDACTED CONFIDENTIAL INFORMATION
REDACTED FROM THIS PUBLIC VERSION

100

Business Unit		Information Protection			
	Milestone 1: Ensure [REDACTED] program meets requirements of all stakeholders and is compliant with CIP Standards	Milestone 2: Ensure that the business unit processes and procedures meet the [REDACTED] requirements <ul style="list-style-type: none"> Each [REDACTED] business unit will document and track the internal controls it has implemented for CIP compliance within its relevant process and procedure documents or [REDACTED] will track all internal controls it has implemented for CIP compliance across all business units and registered entities in a separate document or file. 	Milestone 3: Conduct training on new or revised processes and procedures	Milestone 4: Implement new or revised processes and procedures	Milestone 5: Certify that each business unit and CIP program area is meeting compliance requirements and provide evidence of completion of all milestones <ul style="list-style-type: none"> [REDACTED] will document how each reported noncompliance in the settlement package was mitigated via a mitigation citation document that is organized by Standard and Requirement under CIP Version 5/6 and indicates which milestones in the consolidated Mitigation Plan mitigated and prevented recurrence of the reported noncompliance under each such Standard and Requirement. Reported noncompliance that began under CIP Version 3 will be addressed in the associated CIP Version 5/6 Standard and Requirement indicated by the “V3-V5 Compatibility Tables.”
[REDACTED]	[REDACTED]				
	[REDACTED]				
	[REDACTED]				
	[REDACTED]				
	[REDACTED]				

Attachment 3

The Companies' Mitigation Plan, designated as [REDACTED] to
address the CIP-014-2 violation

This item was signed by [REDACTED] on 7/18/2017

This item was marked ready for signature by [REDACTED] on 7/18/2017

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

A.1 Notices and requirements applicable to Mitigation Plans and this Submittal Form are set forth in "[Attachment A - Compliance Notices & Mitigation Plan Requirements](#)" to this form.

[Yes] A.2 I have reviewed Attachment A and understand that this Mitigation Plan Submittal Form will not be accepted unless this box is checked.

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]
[REDACTED]

Compliance Registry ID: [REDACTED]

B.2 Identify the individual in your organization who will be the Entity Contact regarding this Mitigation Plan.

Name: [REDACTED]

SECTION C: IDENTIFICATION OF ALLEGED OR CONFIRMED VIOLATION(S) ASSOCIATED WITH THIS MITIGATION PLAN

C.1 This Mitigation Plan is associated with the following Alleged or Confirmed violation(s) of Reliability Standard listed below.

Standard:

CIP-014-2

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	[REDACTED]	[REDACTED]	7/11/2016

C.2 Identify the cause of the Alleged or Confirmed violation(s) identified above:

During the fall 2015 CIP-014-2 R1 assessment [REDACTED] an physical security analysis for [REDACTED] stations and [REDACTED] substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. Upon further scrutiny during the week of April 25, 2016, however, it was determined that [REDACTED] Substation had not been run in the final analysis that was shared with the unaffiliated third party verifier for R2. [REDACTED] Substation in both its present and future state was run in preliminary analysis by [REDACTED] and was not found to have adverse results requiring inclusion on the physical security protection list for the purpose of CIP-014-2. Failure to include [REDACTED] in the final analysis shared with the unaffiliated third party verifier, however, may possibly constitute a violation of R2.

[Attachments \(\)](#)

C.3 Provide any additional relevant information regarding the Alleged or Confirmed violations associated with this Mitigation Plan:

This violation was a [REDACTED] PV but is being submitted on the [REDACTED] Portal as a [REDACTED] violation.

[Attachments \(\)](#)

SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

D.1 Identify and describe the action plan, including specific tasks and actions that your organization is proposing to undertake, or which it undertook if this Mitigation Plan has been completed, to correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

In future assessments, run all [REDACTED] stations and substations to be shared with the unaffiliated third party verifier, making no exclusions for Applicability Section 4.1.1. Have the unaffiliated third party verifier a) review all analysis results and b) verify accuracy of [REDACTED] application of Applicability Section 4.1.1 via a [REDACTED] program contingency report using the present-day and 24-months-out base cases as well as the system one-line diagrams.

D.2 Provide the date by which full implementation of the Mitigation Plan will be, or has been, completed with respect to the Alleged or Confirmed violations identified above. State whether the Mitigation Plan has been fully implemented:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

9/30/2016

D.3 Enter Milestone Activities, with due dates, that your organization is proposing, or has completed, for this Mitigation Plan:

1. Run Special Assessment

Milestone Completed (Due: 7/31/2016 and Completed 6/17/2016)

Run [REDACTED] substation in a special assessment and share with the unaffiliated third party verifier.

2. Revisit best practices

Milestone Completed (Due: 9/1/2016 and Completed 8/29/2016)

Revisit CIP 014 2 best practices with [REDACTED]

3. Modify and republish Methodology

Milestone Completed (Due: 9/30/2016 and Completed 9/30/2016)

Modify and republish [REDACTED] CIP 014 2 Methodology to incorporate the proposed approach stated in Section D 1 of the Mitigation Plan.

SECTION E: INTERIM AND FUTURE RELIABILITY RISK

E.1 Abatement of Interim BPS Reliability Risk: While your organization is implementing this Mitigation Plan the reliability of the Bulk Power Supply (BPS) may remain at higher risk or be otherwise negatively impacted until the plan is successfully completed. To the extent they are, or may be, known or anticipated: (i) identify any such risks or impacts; and (ii) discuss any actions that your organization is planning to take to mitigate this increased risk to the reliability of the BPS. (Additional detailed information may be provided as an attachment):

The alleged violation as described in C2 did not at any time impose a higher level of risk on the BPS. As stated previously, [REDACTED] Substation in both its present and future state was run in preliminary analysis by [REDACTED] and was not found to have adverse results requiring inclusion on the physical security protection list for the purpose of CIP-014-2.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitigation Plan will prevent or minimize the probability that your organization incurs further risk of Alleged violations of the same or similar reliability standards requirements in the future. (Additional detailed information may be provided as an attachment):

The mitigating actions described in this mitigation plan will minimize the probability that [REDACTED] incurs further risk or alleged violations of the same nature by ensuring that all Transmission stations and substations are included in the risk assessment analysis that is shared with the third party verifier, making no exclusions for the Applicability Section 4.1.1.

Attachments ()

SECTION F: AUTHORIZATION

An authorized individual must sign and date this Mitigation Plan Submittal Form. By doing so, this individual, on behalf of your organization:

- a) Submits this Mitigation Plan for acceptance by [REDACTED] and approval by NERC, and
- b) If applicable, certifies that this Mitigation Plan was completed on or before the date provided as the 'Date of Completion of the Mitigation Plan' on this form, and
- c) Acknowledges:
 - I am [REDACTED] of [REDACTED]
 - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
 - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
 - I have read and am familiar with the contents of this Mitigation Plan
 - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by [REDACTED] and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

[REDACTED]

Attachment 4

Record documents for the violation of CIP-002-5.1 R1

4.a The Companies' Self-Report [REDACTED]

4.b The Companies' Self-Report [REDACTED]

4.c The Companies' Self-Report [REDACTED]

4.d The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.2.; 1.3.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

Monitoring Method for previously reported or discovered:

On-site Audit

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: [REDACTED]

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

CIP-002-5.1 R1 requires [REDACTED] to implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:
R1.2 requires [REDACTED] to identify each of the Medium Impact BES Cyber Systems according to Attachment 1, Section 2, if any at each asset.

On July 1, 2016, a cyber asset list of devices for [REDACTED] was approved by the CIP Senior Manager. During an [REDACTED] in [REDACTED] a [REDACTED] attending an audit participated in discussions about cyber asset inventory inaccuracies at [REDACTED]. As an additional precaution to determine if the situation applied to [REDACTED] the [REDACTED] performed a comparison of the [REDACTED] BES Cyber Asset list to a list of devices in the [REDACTED] database. A problem with results from an [REDACTED] query was discovered causing two devices to be missed.

The two BES Cyber Asset missing from the approved list creates a possible violation of the [REDACTED] identification of Cyber Assets Enterprise Procedure and NERC CIP standard and requirement CIP-002-5.1 R1.2.

An Apparent Cause Analysis of this possible violation identified the following apparent and contributing causes:

Apparent Cause #1

The [REDACTED] query results for [REDACTED] did not include all relays that are "In Service". This is due to a query script mismatch that was searching for the field to contain "In Service" instead of "In-Service". In-Service with a dash between the words was used in the field for the [REDACTED]

Apparent Cause #2

The inventory list used during the physical walk-down for the [REDACTED] were not compared to the final BES Cyber Asset list generated from [REDACTED] to ensure all required assets were listed. The query results were accepted as a complete list of cyber assets

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Contributing Cause #1

[REDACTED] requires a list of cyber assets after an initial inventory (physical walk-down) is performed. This Cyber Asset inventory is used as an input to the BES Cyber Asset Identification step in the [REDACTED]

This possible violation includes the following BES Cyber Assets:



Are Mitigating Activities in progress or completed? Yes

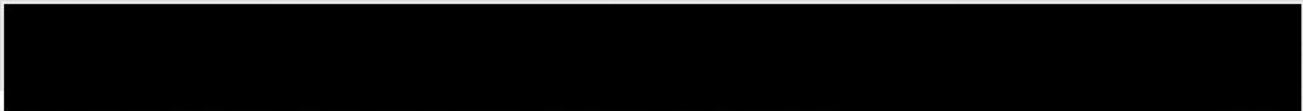
An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Immediate Actions Taken

1. Data entries of "In-Service" in the [REDACTED] database are corrected to match the pick list of "In Service".
2. All query data fields are validated and locked down which results in accurate query results
3. The [REDACTED] BES Cyber Asset List and [REDACTED] BES Cyber Asset List are updated.

Provide details to prevent recurrence:



- [REDACTED] will update the [REDACTED] to include the following:
 - o roles and responsibilities
 - o list of documents needed for walkdown performance including: current [REDACTED] data, current [REDACTED] list data, list of substation cyber-assets to be evaluated, list passwords
 - o record of findings
 - o closeout actions
 - o tracking closeout actions
 - o protocol for addressing findings that could have an imminent compliance impact
 - o required walkdown evidence
 - o acceptable characteristics of evidence including no blanks, legible, dated, location
 - o Record of next, last, and previous walk downs
 - o location for storing walkdown evidence
- [REDACTED] will communicate the [REDACTED] walk-down procedure via email and/or staff meetings to identified personnel.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/30/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the BES cyber assets missing from the approved list have appropriate cyber security controls in place which reduces the risk to the bulk electric system. [REDACTED] CIP-007 security controls that apply to medium impact cyber assets were reviewed and no deficiencies were found.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [REDACTED] on 12/6/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

Monitoring Method for previously reported or discovered:

On-site Audit

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/26/2017

Beginning Date of Possible Violation: 4/17/2017

End or Expected End Date of Possible Violation: 6/26/2017

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

On Monday, June 26 2017, [REDACTED] observed that the BES Cyber Assets [REDACTED] for [REDACTED] were not added to the AIC compliance inventory.

[REDACTED] Initial investigation concluded these BES Cyber Assets were added to the [REDACTED] and were categorized using the Transmission Asset Classification process. Additionally, the default and shared account passwords were changed and the system security baselines were created in accordance with the requirements of CIP-007-6.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Absence of the BES Cyber Assets from the Cyber Asset inventory could cause moderate impact to the Bulk Electric System because without the assets accounted for in the inventory, there is a lack of awareness of them. This lack of awareness and accountability could result in failure to apply necessary security controls to the devices including

password management, malicious code prevention, security baselines, patch management, etc.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Actual Risk to Bulk Power System:

Although the devices were not added to the Cyber Asset inventory, all other security controls were addressed including default password changes, system security baselines, malicious code prevention, etc. Additionally, the devices are not remotely accessible and other required physical access controls were in place to prevent unauthorized physical access to the devices. As a result, there was no Actual Impact to the Bulk Electric System caused by this possible violation because and there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 12/6/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

Monitoring Method for previously reported or discovered:

On-site Audit

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/20/2017

Beginning Date of Possible Violation: 7/16/2017

End or Expected End Date of Possible Violation: 7/21/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Absence of the BES Cyber Assets from the Cyber Asset inventory could cause moderate impact to the Bulk Electric System because without the assets included in the inventory, there is a lack of awareness of them. This lack of awareness and accountability could result in failure to apply necessary security controls to the devices including password management, malicious code prevention, security baselines, patch management, etc.

Provide detailed description of Actual Risk to Bulk Power System:

Although the devices were not added to the Cyber Asset inventory, the devices are not remotely accessible and other required physical access controls were in place to prevent unauthorized physical access to the devices. As a result, there was no Actual Impact to the Bulk Electric System caused by this possible violation because and there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [REDACTED] on 12/11/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 9/19/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 9/21/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-002-5.1a, R1 Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 (High Impact), 1.2 (Medium Impact), 1.3 (Low Impact): iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

In July, 2015 a change was made to the [REDACTED] that folded the [REDACTED] into one (1) island to form the [REDACTED]. The formation of the [REDACTED] changed the Blackstart Resource to [REDACTED] and changed the cranking path element from [REDACTED] to [REDACTED]. Under CIP-002-5.1A, R2 [REDACTED] is obligated to perform a 15 month review of the BES Asset inventory and have the CIP Senior Manager approve the identification of BES Assets. During this review (in September 2017), it was discovered that the [REDACTED] cranking path has been incorrectly shown [REDACTED] on the approved BES Asset inventory since the effective date of CIP Version 5 (July 1, 2016) resulting in a possible violation of the above referenced standard and requirement.

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following: The BES Asset List was updated to account for this change to the Cranking Path.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The purpose of this requirement is to ensure all BES Assets are accounted for to ensure any associated Cyber Assets are afforded appropriate cyber security controls. Since the cranking path was not identified correctly on the BES Asset list, the potential impact to the BES could be moderate, because without awareness and accountability of the BES Asset, any applicable cyber security controls would not be considered or implemented.

Provide detailed description of Actual Risk to Bulk Power System:

The CIP BES Asset list (for cranking path elements) is dependent upon restoration plans required under the NERC O&P standards. And although the [REDACTED] BES Asset list was inaccurate regarding these elements, inclusion of these elements on the list would have no impact on BES reliability because they were identified as BES Assets with NO BES Cyber assets (thus not in CIP Scope). Further, these cranking path elements were identified appropriately in the O&P restoration plan and there has been no Actual Impact to the BES because there were no misoperations, emergencies, or other adverse consequences to the BES.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 5

Record documents for the violation of CIP-003-3 R4

5.a The Companies' Self-Report



5.b The Companies' Self-Report



This item was submitted by [REDACTED] on 9/22/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-003-3

Applicable Requirement: R4.

Applicable Sub Requirement(s): R4.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/30/2015

Beginning Date of Possible Violation: 5/1/2011

End or Expected End Date of Possible Violation: 5/5/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Under NERC CIP requirement for Cyber Security Management Controls - CIP-003-3; R4.1, documentation and classification of information was not met because the NERC-CIP stamp on the [REDACTED] diagrams was missing. Because of the removal of the required stamp, viewers of these documents were not aware of the sensitivity of the Critical Cyber Asset Information and a potential security threat was present if these diagrams were viewed by parties other than those who had authorized access to them.

Description of Event:

On April 30, 2015, while reviewing the [REDACTED] updates at both [REDACTED] and [REDACTED], it was found the existing [REDACTED] drawings were missing the NERC-CIP Stamp. Upon investigation, it was found the stamps were removed during a design project in 2011 by the Drafting Team.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:
1. Replacement of the NERC CIP stamp on both drawings.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:
1. A [REDACTED] checklist which asks the question of whether the drawing has a NERC_CIP stamp on it.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

5/5/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the BES was minimal as even though the drawings were not properly labeled for a period of time, [REDACTED] Additionally, only the parties authorized to view the drawings had them in their possession.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation. Additionally, only the parties authorized to view the drawings had them in their possession.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. The error made by the drafting team member as to the requirements and sensitivity of the drawings was due to inexperience.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue. If the drafting team member was experienced or if a CAD team member completed the drawing, then the violation may not have occurred.

Improvements to the internal compliance plan have been addressed and are being developed as a result of the potential noncompliance .

The circumstances surrounding this violation are the Drafting team's unintentional action of not replacing the NERC CIP stamp on the revised Diagrams during the design phase of the project.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 11/24/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-003-3

Applicable Requirement: [REDACTED]

R4.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 8/11/2015

Beginning Date of Possible Violation: 8/3/2015

End or Expected End Date of Possible Violation: 8/11/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP 003-3 R4, [REDACTED] is obligated to classify and protect information associated with Critical Cyber Assets.

During the conversion from [REDACTED] the parent fileshare (6 folders) used for NERC/CIP drawings was converted to read-only. When this happened the change cascaded down to the children directories and temporarily removed the deny permission on the folders. In this case, all file permissions were set to read only and removed other security permissions that denied access to NERC CIP information. [REDACTED] users had authorized access to the fileshare. When the read only configuration was changed, access to BES Cyber System Information was opened up to all of [REDACTED] BES Cyber Assets potentially impacted are as follows:

This issue was discovered and corrected on 8/11/2015 when a user raised a ticket they could not write to the fileshare. At that time, both the requestor of the change and analyst performing the security change were unaware NERC CIP drawings were on the fileshare. Upon discovery, permissions were restored to the affected folders. Total time lapsed was seven days.

The violation was determined to be self-report for non-compliance with CIP-003-3 R4 since [REDACTED] is expected to control access to information that is identified under a CCAI program

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The actions that [REDACTED] is taking to prevent recurrence include the following:

1. The original permissions were restored to the impacted folders
2. All folders there were targeted for future conversion to read-only were evaluated for CIP impacts. Those that did [REDACTED] were noted and handled in a one off manner to ensure permissions stayed in place on the CIP folder.
3. A peer check was performed afterward to ensure that permissions were still in place.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

All folders there were targeted for future conversion to read-only were evaluated for CIP impacts. Those that did [REDACTED] were noted and handled in a one off manner to ensure permissions stayed in place on the CIP folder.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/11/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because employees were appropriately trained, completed a PRA and were unaware of the incorrect access provisioned to the fileshare. In addition, [REDACTED] has controls in place whereby a quality review is conducted to ensure access has been provisioned as authorized, and the process is not closed out and notifications made of the access being granted to management until this quality review is complete.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. The error made as to the requirements and sensitivity of the NERC CIP documents was due to human error.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue.

The circumstances surrounding this violation are the unintentional actions of not replacing the NERC CIP access permissions during the conversion from [REDACTED]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 6

Record documents for the violation of CIP-003-3 R6

6.a Audit Summary

6.b The Companies' Self-Report

6.c The Companies' Self-Report

6.d The Companies' Self-Report

6.e The Companies' Self-Report

6.f The Companies' Self-Report

Possible Violation (PV) / Find, Fix, and Track (“FFT”) Identification Form

This document is to be completed upon identification of a possible violation (PV), typically within 5 business days of the audit exit brief and emailed to [REDACTED] with a copy to [REDACTED]

For non-FFT candidates: Upon receipt of this document, Enforcement will coordinate with the reporting auditor and Enforcement to initiate the Enforcement processing of this possible violation.

Violation Reported By: [REDACTED]

Submittal Date: [Click here to enter text.](#)

Candidate for FFT Treatment: YES ☐ NO ☒

Registered Entity: [REDACTED]

NERC Registry ID#: [REDACTED]

Compliance Monitoring Process: Compliance Audits

Standard, Version and Requirement in Violation: CIP-003-3 R6

Registered Function(s) in Violation: [REDACTED]

Initial PV Date (Actual Date Discovered by ReliabilityFirst): [REDACTED]

Date for Determination of Penalty/Sanction (Beginning Date of Violation): 9/03/2015

End Date of Possible Violation: Unknown

For Non-FFT Candidate ONLY

Violation Risk Factor: VRF - Medium

Violation Severity Level: Severe VSL

Potential Impact to Bulk Electrical System (BES): Minimal

Provide Explanation for Selection:

██████████ did not follow their established change control process. Also, ██████████ did not follow their implemented cyber security test procedures and did not document test results.

For Non-FFT and FFT Candidates

Basis for the PV:

Several instances of non-compliance were identified where the established change control process was not followed, required cyber security test procedures were not followed and test results were not documented. These instances would be violations of CIP-007-3 R1 (R1,R1.3) and CIP-003-3 R6.

Facts and Evidence pertaining to the PV:

Evidence:

- RSAW CIP-010-2_2015_v1_FINAL.pdf
- RFI-2-032.docx
- RFI-2-041.docx

Facts:

The audit team reviewed the RSAW narrative (*RSAW CIP-010-2_2015_v1_FINAL.pdf*) provided by ██████████ where they made the following statements:

“It was discovered that documentation of the test results, including the differences in the test environment, were not performed. For an example in which the business area has implemented the V5 compliance program, see “Change to Baseline.xlsx” for evidence of testing plan and procedures performed for a change, as well as documentation of verification of results.”
(*RSAW CIP-010-2_2015_v1_FINAL.pdf*, page 16)

The audit team issued RFI-2-032 requesting ██████████ to provide further details regarding the discovery that documentation of the test results, including the differences in the test environment, were not performed. ██████████ responded that “[...] documentation, as it relates to CIP-010 R1.5.2, was not sufficient to evidence testing of successful test results nor were description of measures used to account for differences between test and production.” (*RFI-2-032.docx*)

The audit team issued RFI-2-041 requesting examples of documentation that were not sufficient evidence of testing of successful test results. ██████████ responded with three examples of changes where sufficient evidence of testing and successful test results were not documented. The dates of those changes were 09/03/2015, 10/24/2015 and 10/28/2015. The narrative from *RFI-2-041.docx* for each is as follows:

1. On September 3, 2015, while working a "new install" ticket (46528) for asset ██████████, the SME also installed ██████████ on the supporting server asset ██████████

[REDACTED], however, the proper change control form was not submitted to support the installation of the software on the server.

On the morning on September 4, 2015 while reviewing a [REDACTED] realized that a change had taken place on asset [REDACTED] and that proper change control had not been followed. The [REDACTED] is an automated process that runs 1 time per day and compares the previous day's baselines with the current baselines to determine if there have been any changes. When the anomaly was identified [REDACTED] technician verified the software had been installed without following proper change control prior to installing the new software.

2. On October 24, 2015 [REDACTED] identified several changes to the baseline on asset [REDACTED] and [REDACTED]. An upgrade had been performed on October 23, 2015 to install [REDACTED] for [REDACTED] upgrade [REDACTED] from [REDACTED] [REDACTED]
3. On October 28, 2015 [REDACTED] identified several changes to the baseline on asset [REDACTED]. An upgrade had been performed on October 27, 2015 to install [REDACTED] for [REDACTED], [REDACTED], [REDACTED]

The audit team finds a possible violation for CIP-007-3 R1 (R1,R1.3) and CIP-003-3 R6 due to not following the established change control process, not following required cyber security test procedures and not documenting test results.. The first issue reported occurred on September 3, 2015. Note that the audit is for CIP-010-1 R1 (Part 1.5) as part of the CIP Version 5 Transition Program.

For FFT Candidates ONLY

1. Why did this possible violation pose a minimal risk:

[Click here to enter text.](#)

2. Has Registered Entity mitigated this possible violation: YES ☐ NO ☐
 - a. If yes, describe mitigating actions and state the date that Registered Entity completed the mitigating actions:

[Click here to enter text.](#)

3. Please answer the following questions to determine whether this possible violation constitutes a “clear on its face” FFT candidate or a “close call.” If the answer to any of the following questions is yes, this possible violation will be treated as a “close call.” Otherwise, this possible violation will be treated as a “clear on its face” FFT candidate.

A. Is there any disagreement amongst the audit team on whether the PV is a “clear on its face” or “close call” candidate: YES ☐ NO ☐

a. If yes, explain why:

[Click here to enter text.](#)

B. Does this possible violation reveal a serious shortcoming in registered entity’s reliability-related processes (e.g. a systematic compliance program failure):

YES ☐ NO ☐

a. If yes, explain why:

[Click here to enter text.](#)

C. Are there any additional facts the audit team needs to know in order to comfortably designate this possible violation for FFT treatment: YES ☐ NO ☐

a. If yes, state those facts:

[Click here to enter text.](#)

4. Did audit team inform registered entity that this possible violation qualifies for FFT treatment? YES ☐ NO ☐

a. If so, on what date? [Enter Date.](#)

This item was submitted by [REDACTED] on 6/30/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-003-3

Applicable Requirement: R6.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

1/14/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/10/2016

Beginning Date of Possible Violation: 4/4/2016

End or Expected End Date of Possible Violation: 12/31/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

=This applies to [REDACTED]

Per CIP-003 R6, [REDACTED] is required to establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software. [REDACTED] is also required to implement supporting configuration management activities to identify, control and document all significant entity or vendor-related configurations to hardware and software components of Critical Cyber Assets.

[REDACTED] SME performed the following upgrade on NERC CIP server [REDACTED] without following proper change control:

This issue was identified while [REDACTED] was reviewing an automated report generated from [REDACTED] which had identified that the ILO on the associated server was upgraded the server change ticket did not include an update to the ILO.

[REDACTED] BES Cyber System which contains:

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

[REDACTED]

Provide details to prevent recurrence:

A Root Cause Analysis has also been performed. Future mitigation activities being considered to prevent recurrence include:

[REDACTED]

Develop updated application and asset deployment Job Aid and/or guidance providing detailed instructions for proper execution of [REDACTED] change control activities when working with separate functional groups through:

1. Adoption of Job Aids and/or guidance specific to:

a. [REDACTED]

b. Aligning with [REDACTED] change control requirements. Ensure that all change control triggers are identified and captured.

c. Providing similar rigor as referenced in [REDACTED]

d. Ensuring personnel do not exceed scope of change ticket per [REDACTED]

2. Development of method of conducting work that enforces operational discipline to execute a procedure (i.e. [REDACTED] other HP Techniques, etc.).

Provide overview training for:

1. Updates to [REDACTED] functionality.

2. Application and asset deployment Job Aid and/or guidance.

Enable [REDACTED] to manage volume of work through the following organizational considerations:

1. Allow [REDACTED] to engage with project managers in prioritization of work efforts.

2. Grant [REDACTED] ability to control schedule of work as a part of IT projects.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

12/31/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

The device in question is located within a defined Physical Security Perimeter (PSP) which is restricted to authorized need-to-access individuals and is monitored for unauthorized physical access attempts 24x7x365.

The devices are located within a defined Electronic Security Perimeter (ESP) which is designed to deny access from the outside by default through the use of firewalls, uses explicit access permissions and devices are configured for electronic logging and monitoring for cyber security events. Alerts are sent to the appropriate personnel when detected.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 7/15/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-003-3

Applicable Requirement:

R6.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

11/3/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/6/2016

Beginning Date of Possible Violation: 6/3/2016

End or Expected End Date of Possible Violation: 6/6/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 6/3/2016, [REDACTED] software was installed on one PCA device ([REDACTED] without the proper change documentation. The device is a PCA in an ESP network. This is a NERC Significant Change.

The software change on the device was discovered the next day when it was reported on the [REDACTED] "Installed Software NERC – Detailed Changes Alert Ticket 24979 dated 6/4/16 2:30 AM." A change ticket was put in, approved, and processed on 6/6/2016.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Once the change was discovered by [REDACTED] the analyst initiated a change control ticket and completed the security controls testing [REDACTED] (68260).

A Root Cause Analysis (RCA) is being performed with the objective to identify other potential mitigating controls to prevent future reoccurrences.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include steps that will be outlined in a change control RCA that is in progress now.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

6/6/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the device was afforded the protection of a secured Electronic Security Perimeter (ESP) and a secured Physical Security Perimeter (PSP). Additionally, once the incident was discovered, mitigating steps were taken to implement change control process via a change control ticket that executed the appropriate security controls testing [REDACTED] ticket #68260).

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 8/10/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-003-3

Applicable Requirement:

R6.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

7/15/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 3/10/2016

Beginning Date of Possible Violation: 3/8/2016

End or Expected End Date of Possible Violation: 5/23/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Issue 1

Applies to [REDACTED]

Date discovered – 3/8/2016

Beginning Date – 3/10/2016

End date of PV – 7/20/2016

On March 8, 2016 @ 14:56 Service Desk ticket 64971 was created in [REDACTED] to install the [REDACTED] agent on [REDACTED] however, 2 NERC CIP assets were not included on the asset links tab within the change ticket. The asset links tab is used to associate assets to the change and if the assets are identified as NERC CIP, the appropriate security controls (SCT) workflow is initiated.

Through additional investigation it was determined that the SME failed to answer three questions correctly on the change control ticket which would have identified the assets as being NERC CIP when the change ticket was created in [REDACTED]. In this potential violation the SME answered NO to the first question which prevented security controls testing workflow from being initiated. Those 3 questions are:

Question #1: Does this change affect an application or system that must adhere to regulatory compliance guidance (e.g. NERC CIP)?

Question #2: Does this change render an application or service unavailable that is considered critical by the business or critical for Business Continuity Planning (BCP)?

Question #3: Does this change have significant downstream impacts on other applications or systems?

Upon further investigation it was determined that testing was not performed on any of the [REDACTED] assets identified on change ticket 64971 because the first question was answered NO.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Date discovered – 5/21/2016
Beginning Date – 5/20/2016

CIP-007-3a R1: The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls.

May 21, 2016, while performing daily change control validations, [REDACTED] determined that changes were detected by [REDACTED] on [REDACTED] for updates that occurred to the [REDACTED] showing an update from [REDACTED] outside of the normal change control workflow.

The original change ticket (67229) included [REDACTED] and was submitted to support changes to the [REDACTED] however this asset [REDACTED] was not included on the original ticket.

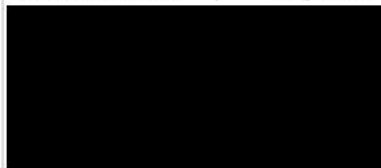
The upgrade to the [REDACTED] included on [REDACTED] ticket 67229 was completed on 5/21/2016. The [REDACTED] report which identified the anomaly on ran at 02:30 on 5/22/2016.

[REDACTED] performed their review of the [REDACTED] report on 5/23/2016 and notified CIP Compliance Lead of the potential violation on the same day at approximately 14:10 EDT.

Service Desk ticket 67942 was submitted on 5/23/2016 to document the change for this asset.

Testing was performed on [REDACTED] ticket 10275 on 06/27/2016 at 14:47:25 with no adverse effects to existing cyber security controls.

It was determined that human error was the cause of this potential violation. The SME responsible for performing the upgrade did not verify that all assets being upgraded were included on the [REDACTED] change ticket.



Are Mitigating Activities in progress or completed? ☒ Yes

If Yes, Provide description of Mitigating Activities:

Issue 1

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

6/29/2016: Change ticket 68764 / Security Controls ticket 10490 have been submitted in [REDACTED] and testing on the identified devices has been initiated.

7/20/2016 testing has been completed on all identified assets.

Issue 2

Testing was performed on [REDACTED] ticket 10275 on 06/27/2016 at 14:47:25 with no adverse effects to existing cyber security controls.

Provide details to prevent recurrence:

Issue 1

The actions that [REDACTED] is taking to prevent recurrence include the following:

6/29/2016: Change ticket 68764 / Security Controls ticket 10490 have been submitted in [REDACTED] and testing on the identified devices has been initiated.

Additionally, a Root Cause Analysis (RCA) is underway that will drive out other mitigating activities that should prevent a [REDACTED] **PROTECTED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

A Root Cause Analysis has also been performed. Future mitigation activities being considered to prevent recurrence include:

Implement the following changes/updates to [REDACTED]

1. Add checkbox ("Initiate Change") in [REDACTED] to indicate that all updates have been made to ticket and security controls testing can run.

Develop updated application and asset deployment Job Aid and/or guidance providing detailed instructions for proper execution of [REDACTED] change control activities when working with separate functional groups through:

1. Adoption of Job Aids and/or guidance specific to:
 - a. Data collection efforts (i.e. mapping data between a Change Request (CRQ) and [REDACTED])
 - b. Aligning with [REDACTED] change control requirements. Ensure that all change control triggers are identified and captured.
2. Development of method of conducting work that enforces operational discipline to execute a procedure (i.e. "Circle Slash" procedure, other HP Techniques, etc.).

Provide overview training for:

1. Updates to [REDACTED] functionality.
2. Application and asset deployment Job Aid and/or guidance.

Enable [REDACTED] to manage volume of work through the following organizational considerations:

1. Allow [REDACTED] to engage with project managers in prioritization of work efforts.
2. Grant [REDACTED] ability to control schedule of work as a part of IT projects.

Issue 2

A Root Cause Analysis has also been performed. Future mitigation activities being considered to prevent recurrence include:

Implement the following changes/updates to Footprints:

1. Add checkbox ("Initiate Change") in Footprints to indicate that all updates have been made to ticket and security controls testing can run.

Develop updated application and asset deployment Job Aid and/or guidance providing detailed instructions for proper execution of [REDACTED] change control activities when working with separate functional groups through:

1. Adoption of Job Aids and/or guidance specific to:
 - a. Data collection efforts (i.e. mapping data between a Change Request (CRQ) and [REDACTED])
 - b. Aligning with [REDACTED] change control requirements. Ensure that all change control triggers are identified and captured.
2. Development of method of conducting work that enforces operational discipline to execute a procedure (i.e. "Circle Slash" procedure, other HP Techniques, etc.).

Provide overview training for:

1. Updates to [REDACTED] functionality.
2. Application and asset deployment Job Aid and/or guidance.

Enable [REDACTED] to manage volume of work through the following organizational considerations:

1. Allow [REDACTED] to engage with project managers in prioritization of work efforts.
2. Grant [REDACTED] ability to control schedule of work as a part of IT projects.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

12/31/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Issue 1

The Potential Impact to the Bulk Power System is minimal because testing has been performed on other assets that had [REDACTED] installed and no negative impact was identified. In addition physical access to the identified devices is limited to NERC CIP trained and authorized personnel and [REDACTED]

Additionally, once the incident was discovered, mitigating steps were taken to implement the documented change control process via a change control ticket which executed the appropriate security controls testing on the identified in scope assets (Security Controls ticket 10490).

Issue 2

The Potential Impact to the Bulk Power System is minimal because testing has been performed on other assets that had [REDACTED] installed and no negative impact was identified.

In addition physical access to the identified devices is limited to NERC CIP trained and authorized personnel and [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

Issue 1

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Issue 2

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

Issue 1

The devices in question are located within a defined Physical Security Perimeter (PSP) which is restricted to authorized need-to-access individuals and is monitored for unauthorized physical access attempts 24x7x365.

Devices are located within a defined Electronic Security Perimeter (ESP) which is designed to deny access from the outside by default through the use of firewalls, uses explicit access permissions and devices are configured for electronic logging and monitoring for cyber security events. Alerts are sent to the appropriate personnel when detected.

Issue 2

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [REDACTED] on 8/31/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-003-3

Applicable Requirement: [REDACTED]

R6.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

11/19/2015

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Report

Has the scope of the Possible Violation expanded: [REDACTED]

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

3/10/2016

Beginning Date of Possible Violation: [REDACTED]

3/5/2015

End or Expected End Date of Possible Violation: [REDACTED]

11/19/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]


Per CIP-003-3 R6 [REDACTED] is obligated to maintain an established and documented process of change control and configuration management for adding, modifying, replacing, or removing Bulk Electric System (BES) Cyber Asset hardware or software. [REDACTED] has implemented supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of BES Cyber Assets pursuant to the change control process.

On 3/10/16, while reviewing Change Management artifacts, [REDACTED] NERC CIP Compliance Analyst discovered the required documentation associated with [REDACTED] was not identified. All required compliance tasks were completed; however, documentation to meet compliance with CIP-003-3 R6 was found to be insufficient.

On 3/14/16, NERC CIP Compliance and [REDACTED] teams met to discuss the potential change control violation. Cause Analysis was performed. During the discussion it was determined further review of [REDACTED] compliance assets was necessary as part of the Extent of Condition to determine the full scope of the potential violation.

The [REDACTED] System Owner and Team performed a comprehensive review of [REDACTED] Asset Inventory and change management documentation

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The mitigating activities [REDACTED] has taken or plans to take with respect to this issue include the following:

1. Notification was made to [REDACTED] Team and System Owner of the issue.
2. Evidence has been compiled showing:
 - Baselines created
 - Testing performed
3. Apparent Cause Analysis to be performed with [REDACTED] Team and [REDACTED]

Provide details to prevent recurrence:

A formal corrective action plan investigation will take place over the next several weeks and from that, mitigating activities and details to prevent recurrence will be identified.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/19/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the BES is minimal because change control steps were completed as dictated by the program; only documentation was omitted. Additionally, these assets are no longer considered critical cyber assets and are now classified as low impact.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. The errors made as to the requirements and completion of change management documentation was due to human error.

[REDACTED] was attempting to comply in good faith with NERC CIP-003-3 R6. The circumstances surrounding this violation are the unintentional actions of failing to complete compliance documentation. Required compliance tasks were performed; however, documentation to meet compliance with the standard was found to be insufficient.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 8/8/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-003-3

Applicable Requirement:

R6.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 9/12/2016

Beginning Date of Possible Violation: 5/20/2015

End or Expected End Date of Possible Violation: 10/31/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

NERC CIP Standard and Requirement:
CIP-003-3

Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

On 05/20/2015 a relay [REDACTED] at [REDACTED] was replaced at with a new [REDACTED] due to an equipment failure. This was discovered during an annual CIP Walk Down on 9/12/2016.

Are Mitigating Activities in progress or completed? Yes

An Informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Protection and Controls Engineering have ensured that these devices met an existing baseline by providing documentation that showed they complied with an existing baseline using methods of collecting information and screenshots on 10/31/2016

Provide details to prevent recurrence:

An Enterprise Change Process has been developed. With leadership support, broad adoption of this change control process will be implemented by 2017.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

10/31/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation. [REDACTED] senior management and direct managers relevant to the situation actively participated and encouraged employees to provide complete information.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 7

Record documents for the violation of CIP-004-3a R2

7.a The Companies' Self-Report



This item was submitted by [REDACTED] on 8/5/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R2.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/4/2016

Beginning Date of Possible Violation: 2/3/2016

End or Expected End Date of Possible Violation: 3/1/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Per CIP-004-3a R2 [REDACTED] is obligated to establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

[REDACTED] was in the process of phasing in a new [REDACTED]. While rolling out this new tool, [REDACTED] determined it would be valuable to ensure the users being added to the new system were compliant with their trainings.

On February 5, 2016, [REDACTED] performed the analysis to determine if there were users with out-of-date trainings, or no trainings altogether. On February 5, [REDACTED] identified nineteen users missing compliant trainings[1,2,3]. [REDACTED] sent communications on February 5 to the gaped individuals informing them they must complete their gap trainings[1,2,3] by February 29, or their access would be revoked.

On February 17, 2016, additional users came into scope for the roll out of the new tool. [REDACTED] performed the same gap analysis on the newly in scope users. Eleven additional individuals were identified on February 17 to require more training than they currently had. The new gaped individuals were contacted on February 17, advising them to complete their outstanding trainings, or their access would be revoked on February 29, 2016.

All individuals completed their trainings with the exception of four. Access for these four individuals was revoked on the following dates: 2/4/2016, 2/17/2016, 2/26/2016, and 3/1/2016.

[REDACTED] is currently evaluating the number of Critical Cyber Assets these users had access to.

[1] [REDACTED] - This introductory course provides information about [REDACTED] NERC CIP Cyber Security Program and the requirements and controls that the company has adopted to protect its critical infrastructure including: cyber security policies, proper handling of device information and its storage, and Identification of a Cyber Security Incident and initial notification / response in accordance with [REDACTED] incident response plan.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[2] [REDACTED] - This course provides guidelines on ports and service management, electronic and remote access management and aims to define Electronic Security Perimeters / Access Points, initiate the necessary activities for Electronic Access Control, Cyber security risks associated with an applicable device's electronic inter-connectivity and interoperability with other applicable devices and outline how to access BES Cyber Assets remotely by using multi-factor authentication.

[3] [REDACTED] - This course is mandatory for [REDACTED] employees whose work requires one to have authorized, unescorted physical access to defined Physical Security Perimeters. This course provides an outline of the visitor control program, guidelines for security monitoring and logging, access management and review and aims to define physical access controls, the visitor control program, outline the proper procedure for entering a Physical Security Perimeter (PSP), the procedures / expectations of an escort, populating the Manual Log, what constitutes as "suspicious activity" and how to report it, protocol if the Physical Access Control System (PACS) experiences an outage and alternative measures during an outage.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

All users had until February 29 to gain compliance with their outstanding trainings. Any users who had not completed the role based mandatory trainings by February 29 had that role removed from their user profile therefore removing their access.

[REDACTED] is currently performing a Direct Cause Analysis to determine the necessary Mitigating Activities to properly mitigate this issue to prevent recurrence.

Provide details to prevent recurrence:

[REDACTED] has built and implemented a new access tool to manage access requests. This tool will not allow users to gain access without the appropriate trainings completed, and will generate tickets for the removal of users' access if they do not complete their yearly trainings as they are required.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

2/29/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal. Although there were a number of users with out-of-date trainings, all users in question, had, at a minimum an up-to-date Personnel Risk Assessment on file, and in all but 2 cases, had up-to-date CIP Program Basics courses on file, showing that at the very least all users had background checks on file.

Provide detailed description of Actual Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal. Although there were a number of users with out-of-date trainings, all users in question, had, at a minimum an up-to-date Personnel Risk Assessment on file, and in all but 2 cases, had up-to-date CIP Program Basics courses on file, showing that at the very least all users had background checks on file.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 8

Record documents for the violation of CIP-004-6 R2

8.a The Companies' Self-Report

8.b The Companies' Self-Report

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

2.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered:

No

Has this Possible Violation previously been reported to other Regions:

No

Date Possible Violation was discovered: 3/31/2017

3/31/2017

Beginning Date of Possible Violation: 3/8/2017

3/8/2017

End or Expected End Date of Possible Violation:	4/1/2017
---	----------

4/1/2017

Is the violation still occurring?	No
-----------------------------------	----

No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to

On 3/8/2017, the

There was one employee in the batch who did not satisfy the training pre-requisites and was consequently granted read-only access to the passwords for

The issue was identified by the [REDACTED] project team preparing for a May release and reconciling training data with role requirements in [REDACTED] on 3/31/2017. When the [REDACTED] was made aware of the issue with the employee having access without the appropriate training, the access was removed that day.

Are Mitigating Activities in progress or completed?	No
---	----

No

Potential Impact to the Bulk Power System:	Moderate
--	----------

Moderate

Actual Impact to the Bulk Power System:	Minimal
---	---------

Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate, due in part to the

A lack of understanding of the responsibilities could result in inappropriate use of the passwords associated with the cyber assets, such as credential sharing with

unauthorized personnel.
Mitigating factors include:

- A valid Personal Risk Assessment
- Immediate removal of the inappropriate access when it was discovered on 3/31/2017

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 6/19/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-004-6

Applicable Requirement: [REDACTED]

R5.

Applicable Sub Requirement(s): [REDACTED]

5.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/28/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 4/28/2018

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]. A removal request was submitted in [REDACTED] on June 8th, 2016 by a [REDACTED] team member to remove three NERC CIP locations for a worker due to his training expiring.

During the 1st Quarter 2017 Quarterly Review, it was discovered that one of the locations associated with the worker's badge, [REDACTED] (high risk asset, one worker), the [REDACTED] (high risk asset, three workers), and the [REDACTED] (medium risk asset, one worker). All five workers' badges had access that should have been removed. Removal requests were submitted and processed for these additional five workers and completed on May 1st, 2017.

While performing an extent of condition (EOC) review, five additional workers were discovered whose physical access had not been properly removed from three sites – the [REDACTED] (high risk asset, one worker), the [REDACTED] (high risk asset, three workers), and the [REDACTED] (medium risk asset, one worker). All five workers' badges had access that should have been removed. Removal requests were submitted and processed for these additional five workers and completed on May 1st, 2017.

In each case, the initial request to remove access was not properly processed by validating that the access had been removed in [REDACTED] (which is a manual process). Furthermore, the Quarterly Review process for identifying, researching, and resolving discrepancies was not followed by a [REDACTED] team member. Access was removed in [REDACTED] but that does not actually remove the access in the end system.

The inappropriate access was not used between the original request to remove and the date the access was actually removed.

The remaining [REDACTED] Project activities will be completed by May 20, 2017.

A cause analysis will take place to assist in preventing recurrence of this possible violation.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is high, due to the severe impact rating for the [REDACTED] involved.

Inappropriate access on a badge could lead unauthorized changes or a disruption of daily operations within the facility due to negligent or malicious activity.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Mitigating factors include:

- Removal of the inappropriate access
- Valid PRA for the six workers
- Valid training for five of the six workers (the initial worker's training was expiring, which led to the initial request)
- The inappropriate access was not used between the original request to remove and the date the access was actually removed

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 9

Record documents for the violation of CIP-004-3a R3

9.a The Companies' Self-Report [REDACTED]

9.b The Companies' Expansion of Scope Assessment [REDACTED]

This item was submitted by [REDACTED] on 7/21/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R3.

Applicable Sub Requirement(s): R3.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

2/10/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 3/31/2015

Beginning Date of Possible Violation: 11/13/2014

End or Expected End Date of Possible Violation: 6/30/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-004-3a R3.2, each personnel risk assessment (PRA) is supposed be updated at least every seven (7) years after the initial personnel risk assessment or for cause. [REDACTED] tracks PRA information within the [REDACTED]. The [REDACTED] group is responsible for requesting the PRAs and validating CIP training is current. The [REDACTED] group exports the information from the [REDACTED] and validates at least monthly that PRAs are current and to ensure that no one has been missed.

However, when this activity was performed on November 13, 2014, one individual was accidentally omitted from the list of PRA requests. This omission was discovered on March 31, 2015, when other CIP compliance monitoring activities were being performed related to NERC personnel risk assessments. The individual who was missed was from the [REDACTED] organization and had NERC unescorted access to two (2) physical security perimeters (PSPs) on his badge along with electronic access to [REDACTED] cyber assets. His last PRA was completed on November 12, 2007.

The employee was inadvertently left off of the list to complete a re-screening which was due on November 12, 2014. He was notified on the day the error was discovered (i.e., March 31, 2015). The re-screening form was submitted that day and the new screening was completed April 01, 2015.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The re-screening form was submitted the day the omission was discovered and the new screening was completed April 01, 2015. The PRA record for this individual has now been updated in [REDACTED]. The omission of this one individual's PRA was just an oversight and not intentional.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide details to prevent recurrence:

[REDACTED] will continue its current practice of requesting personnel risk assessments (PRAs) as required by the standards and also continue its verification process to ensure that no PRAs are omitted in the future.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/1/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal. The employee involved with this issue was current on his required CIP training and the PRA was requested and completed immediately upon discovery of this issue.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation. There were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of an intentional action to violate a NERC reliability standard. Rather, [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard. It is evident that [REDACTED] was attempting to comply as evidenced by the additional personnel risk assessment performed after the discovery of the issue.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

DOCUMENT TYPE	DOCUMENT	LAST ACTION
DATE	EVENT	USER
<input checked="" type="checkbox"/> 7/30/2018	Request for Settlement Discussions: Document Withdrawn by Region	
<input checked="" type="checkbox"/> 6/30/2016	Request for Settlement Discussions: Initial Document Creation (Region)	
<input checked="" type="checkbox"/> 6/30/2016	Request for Settlement Discussions: Region Sent Document to NERC	
<input checked="" type="checkbox"/> 6/27/2016	Request for Settlement Discussions: Region Received Document From Registered Entity	
<input checked="" type="checkbox"/> NPV: Notice of Possible Violation	CONFIDENTIAL [REDACTED].pdf (29.79 KB)	06/03/2016 Region Sent Document to Registered Entity
DATE	EVENT	USER
<input checked="" type="checkbox"/> 6/3/2016	NPV: Notice of Possible Violation: Region Sent Document to Registered Entity	
<input checked="" type="checkbox"/> 6/3/2016	NPV: Notice of Possible Violation: Initial Document Creation (Region)	
<input checked="" type="checkbox"/> 6/3/2016	NPV: Notice of Possible Violation: Region Sent Document to NERC	
<input checked="" type="checkbox"/> Request for Additional Information		09/11/2015 Region Sent Document to Registered Entity
DATE	EVENT	USER
<input checked="" type="checkbox"/> 9/11/2015	Request for Additional Information: Region Sent Document to Registered Entity	
<input checked="" type="checkbox"/> 9/11/2015	Request for Additional Information: Initial Document Creation (Region)	

Entity Documents

DOCUMENT TYPE	DOCUMENT	LAST ACTION
---------------	----------	-------------

Related Violations

Violation History

CATEGORY	REGION ID	NERC VIOLATION ID	DATE REPORTED	REQUIREMENT	POINT OF CONTACT	VIOLATION STATUS	SELF-LOG	FINAL FILING MECHANISM
----------	-----------	-------------------	---------------	-------------	------------------	------------------	----------	------------------------

Related Violations

Parent Violation

Child Violations

REGION ID	NERC VIOLATION ID	REQUIREMENT	DATE REPORTED	POINT OF CONTACT	VIOLATION STATUS
-----------	-------------------	-------------	---------------	------------------	------------------

Scope Expansions

REGIONAL SCOPE EXPANSION ID	STATUS
20	12/22/2015 Scope Expansion Accepted

Summary

Date possible violation expansion was discovered:

8/6/2015

REGIONAL SCOPE EXPANSION ID

STATUS

Beginning date of new expansion of possible violation:

5/19/2015

End or expected end date of new expansion of possible violation:

8/11/2015

Detailed description and cause of possible violation:

Applies to

In May, 2015 two individuals with NERC badge access (one of whom also had NERC electronic access) were not notified to complete their seven-year PRA renewal before the expiration dates (5/19/15 and 5/26/15).

The error was discovered on 8/6/2015. Therefore, a compliance gap occurred from 5/19/2015 to 8/6/2015 during which time the employees had electronic access to 2 (two) groups and physical access to

The incident was discovered during a review of training data in the HR Workforce Hub and PRAs being received and processed by

Immediate corrective action was performed - NERC badge access and electronic access were removed. PRAs were renewed.

Are Mitigating Activities in progress or completed?

Yes

Date Mitigating Activities are expected to be completed:

8/11/2015

Description of Mitigating Activities:

Immediate corrective action was performed. NERC badge access and electronic access was removed on 8/6/2015. PRAs were renewed on 8/10/2015 and 8/11/2015.

Details to Prevent Recurrence:

is performing a cause analysis to determine the root cause behind the issue. The cause analysis will suggest potential activities to prevent reoccurrence. Corrective action approved by management will be implemented to prevent reoccurrence.

Actual Impact to the bulk power system:

Minimal

Initial Reliability Impact Statement:

The Potential Impact to the Bulk Power System is minimal because the employee involved with this issue was current on his required CIP training and the PRA was requested immediately and renewed upon discovery of this issue.

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Entity Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

Review

Review Date:

1/5/2016

Reviewer:

Review Findings:

Accepted

Reviewer Notes or Comments:

To be considered during determination

Attachment 10

Record documents for the violation of CIP-004-3 R6

10.a The Companies' Self-Report [REDACTED]

10.b The Companies' Self-Report [REDACTED]

10.c The Companies' Self-Report [REDACTED]

10.d The Companies' Self-Report [REDACTED]



on 8/31/2016



Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-3a

Applicable Requirement:

R3.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/5/2016

Beginning Date of Possible Violation: 6/30/2016

End or Expected End Date of Possible Violation: 7/5/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to

Per CIP-004-5.1, R3.5, is obligated to have a process to Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years..

On 6/29/2016, a manager entered a request in the system for a contractor to have NERC badge access to 3 PSPs:

1. PSP ACCESS
2. PSP ACCESS
- 3.

The work items were processed on 6/30/2016 and the badge access was set up as requested. On 7/5/2016, it was discovered that the contractor's Personnel Risk Assessment (PRA) was expiring; The contractor's PRA was confirmed to have been last completed on June 30, 2009.


At the time that the request was made, the PRA for this worker had not expired and work items were issued for to provision access.

The contractor previously had NERC access but that access was removed in December 2015. Subsequently, when the lists of those who needed to be re-screened were reviewed to determine if a new PRA was needed, the contractor's name was not on the list because she had no active NERC access at that time.

The contractor did not access any of the 3 PSPs she had been authorized for between 6/30/2016 – 7/5/2016.

The contractor completed CIPBASIC, NERC CIP Cyber Security Program training on 4/26/2016.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Access to PSPs was removed 7/5/2016 and started process for having a Personnel Risk Assessment performed.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:
Perform research to add logic to the [REDACTED] system for PRA and CIP training expirations.
Process improvement
Updated existing procedures for PRA expiration checks
Updates planned will include steps to identify and notify individuals with expiring PRAs of their PRA expiration date and the need to have the PRA renewed if future NERC CIP access will be requested.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because the individual had the potential to access 2 PSPs without an active/approved Personnel Risk Assessment in place. The third PSP site that was authorized, [REDACTED] SUBSTATION, was out of scope.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

[REDACTED] on 5/22/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-6

Applicable Requirement: R3.

Applicable Sub Requirement(s): 3.5.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/24/2017

Beginning Date of Possible Violation: 4/16/2017

End or Expected End Date of Possible Violation: 4/24/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED] only.

The [REDACTED] team has the responsibility of creating lists of workers who have CIP access, sending reminders to those workers and managers, monitoring those workers, and removing access.

On Monday, February 20, 2017, the [REDACTED] began sending out notifications to workers whose Personal Risk Assessments (PRAs) were going to expire in preparation for a change in classification to the [REDACTED]

There was a misunderstanding between the [REDACTED] team regarding which team would be doing the monitoring and removal of access if a PRA was coming close to expiration and a worker had access. [REDACTED]

During the Quarterly Review, a member of the [REDACTED] team discovered a worker who no longer had a valid PRA in the [REDACTED] application. The worker had access to [REDACTED]. The worker's PRA expired on April 16, 2017. The lack of a valid PRA was discovered on April 24, 2017, and removal of all CIP access occurred on April 25, 2017.

While performing an extent of condition review of all workers who have electronic or physical access in [REDACTED] against PRA records, another worker whose PRA also expired on April 16, 2017 was discovered and his access was removed on April 25, 2017 as well. [REDACTED]

The workers were sent emails on the dates listed below informing them that their PRAs were going to expire on April 16, 2017:

- February 20, 2017
- March 13, 2017
- April 3, 2017

The [REDACTED] team has been conducting daily checks for PRA expiration since April 26, 2017 and will continue until the [REDACTED] implements the new [REDACTED] tool on May 13, 2017.

Upon implementation of the [REDACTED] application on May 13, 2017, [REDACTED]

The remaining [REDACTED] activities will be completed by May 20, 2017.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate, due in part to the medium impact rating for the [REDACTED]

An expired PRA could result in "Insider threat" risk or inappropriate access or changes to an asset.

Mitigating factors include:

- Valid NERC CIP training
- Removal of the inappropriate access

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
---	----

No

Has this Possible Violation previously been reported to other Regions:	No
--	----

No

Date Possible Violation was discovered: 1/5/2017

1/5/2017

Beginning Date of Possible Violation: 7/1/2016

7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

1/11/2017

Is the violation still occurring? No

No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to
In January 2017.

Are Mitigating Activities in progress or completed?	Yes
---	-----

Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

a. [REDACTED] - 74357 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
b. [REDACTED] - 74363 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
c. [REDACTED] - 74355 - Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)



on 1/23/2018



Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

4/7/2017

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: Yes

If yes, indicate which Region(s):

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED] and [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby [REDACTED] determine the function of a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Method of Discovery

Self-Assessment: [REDACTED]

Extent Of Condition:

As part of the [REDACTED] Refresh Program the [REDACTED] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with the [REDACTED] Refresh Program and 2) ensure [REDACTED] Level processes support the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [REDACTED] requirements of the process, no process available.

Cause Identification:

Are Mitigating Activities in progress or completed? ☒ Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar PRR/NERD and CONFIDENTIAL. INFO

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System:	Moderate
--	----------

Actual Impact to the Bulk Power System:	Minimal
---	---------

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:

Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The [REDACTED] internal compliance plan was in effect at the time of the potential noncompliance. [REDACTED] management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section

Attachment 11

Record documents for the violation of CIP-004-3a R4.2

- 11.a Audit Summary [REDACTED]
- 11.b The Companies' Self-Report [REDACTED]
- 11.c The Companies' Self-Report [REDACTED]
- 11.d The Companies' Self-Report [REDACTED]
- 11.e The Companies' Expansion of Scope Assessment [REDACTED]
- 11.f The Companies' Self-Report [REDACTED]
- 11.g The Companies' Self-Report [REDACTED]
- 11.h The Companies' Self-Report [REDACTED]

Possible Violation (PV) / Find, Fix, and Track (“FFT”) Identification Form

This document is to be completed upon identification of a possible violation (PV), typically within 5 business days of the audit exit brief and emailed to [REDACTED] with a copy to [REDACTED]

For non-FFT candidates: Upon receipt of this document, Enforcement will coordinate with the reporting auditor and Enforcement to initiate the Enforcement processing of this possible violation.

Violation Reported By: [REDACTED]

Submittal Date: [REDACTED]

Candidate for FFT Treatment: YES ☐ NO ☒

Registered Entity: [REDACTED]

NERC Registry ID#: [REDACTED]

Compliance Monitoring Process: Compliance Audits

Standard, Version and Requirement in Violation: CIP-004-3a R4.2

Registered Function(s) in Violation: [REDACTED]

Initial PV Date (Actual Date Discovered by [REDACTED] : [REDACTED]

Date for Determination of Penalty/Sanction (Beginning Date of Violation): 4/30/2015

End Date of Possible Violation: Unknown

For Non-FFT Candidate ONLY

Violation Risk Factor: VRF - Medium

Violation Severity Level: Moderate VSL

Potential Impact to Bulk Electrical System (BES): Moderate

P [REDACTED] **Selection:**
[REDACTED] did not revoke access to Critical Cyber Assets within 24 hours for an employee terminated for cause.

For Non-FFT and FFT Candidates

Basis for the PV:

A review of personnel sampling evidence detected an employee terminated for cause did not have their access revoked within 24-hours.

Facts and Evidence pertaining to the PV:

Evidence:

- [REDACTED]
- [REDACTED]
- [REDACTED] Access Removal.docx
- [REDACTED].docx
- [REDACTED] HR Changes and Physical Access.docx
- [REDACTED] HR Changes and Electronic Access Removal.docx
- [REDACTED] HR Changes and Electronic Access Removal.docx
- [REDACTED] Termination Account Deactivation.docx
- Q2 Reviews and Q3 Reviews (these are IT folders that contains multiple files of quarterly access reviews)

Facts:

The audit team issued RFI-1-010 requesting [REDACTED] to provide evidence of quarterly reviews of lists of personnel who have specific electronic and/or physical access rights to CCAs as well as provide evidence of these lists being updated within 7 calendar days of any change of personnel or any change of access rights of such personnel. [REDACTED] provided [REDACTED] as narrative files for the quarterly access reviews of electronic and physical access under the [REDACTED] areas and updating the access lists within the allotted timeframe.

The audit team reviewed the access removal for [REDACTED] who was terminated 'For Cause'. [REDACTED] showed [REDACTED] ticket was entered on 4/2/2015 to remove [REDACTED] electronic access but his access was not deactivated until 4/7/2015. The [REDACTED] ticket did not indicate the termination was 'For Cause'.

Open Enforcement Actions:

- [REDACTED] and [REDACTED]
[REDACTED] Discovered 7/24/15. Occurred 7/17/15.
- NERC Access Services personnel approved access request in error for a contractor.

- [REDACTED] Discovered 5/19/14; Occurred 12/20/13.
- Student employee PSP access was not fully revoked prior to being reinstated upon return now not requiring PSP access.

Recommendations:

The audit team also found that improvements are needed for [REDACTED] process documentation and processing access removals. The recommendations, in general, are to strengthen [REDACTED] by implementing additional controls to ensure access removal is performed in a timely manner (including employees, vendors and contractors), monitored, tracked and recorded appropriately.

The following recommendations were communicated to [REDACTED] to further enhance their program:

- Include the date the access review was performed within the Quarterly Access Review spreadsheets and ensure that all cells are completed including the specific date of the initiating event (rather than the latter date of when the [REDACTED] ticket is created to remove the access).
- For third party service providers (contractors and vendors), ensure appropriate documentation is collected to substantiate the date of the initiating event in comparison to the access removal date within the [REDACTED] ticket.
- Appropriate documentation must be collected as part of the ticket to document the date/time of the “initiating” event. For example, the audit team sampled several personnel for which [REDACTED] provided evidence of the help desk ticket to remove access. [REDACTED] measured compliance using the start date/time in the ticket against the end date/time of the ticket to demonstrate compliance to the seven (7) day and/or twenty-four hour (24) requirement. Though [REDACTED] processes requests via help desk tickets, they do not record and document the “initiating action” and associated date/time which generates the access removal request. Similarly, [REDACTED] stated that they rely on vendors and contractors to create a ticket in their system in a timely manner but does not substantiate, audit or monitor third party contractors or vendor firms to ensure that requests are being processed within the required seven (7) days or twenty-four (24) hour compliance timeframe(s).
- [REDACTED] also stated that they do not monitor or assess access removals in between the quarterly access reviews. It is recommended that [REDACTED] implement a process to coordinate with HR periodically review personnel change and terminations to ensure managers are submitting and processing requests in a timely manner. This may include coordinating with HR to identify the specific dates and records of personnel (with such access to Critical Cyber Assets) transfer and/or terminations.

The audit team finds a possible violation for CIP-004-3 R4 (R4.2) as [REDACTED] did not revoke access to Critical Cyber Assets within 24 hours for an employee terminated for cause.

1. Why did this possible violation pose a minimal risk:

[Click here to enter text.](#)

2. Has Registered Entity mitigated this possible violation: YES ☐ NO ☐
 - a. If yes, describe mitigating actions and state the date that Registered Entity completed the mitigating actions:

[Click here to enter text.](#)

Please answer the following questions to determine whether this possible violation constitutes a “clear on its face” FFT candidate or a “close call.” If the answer to any of the following questions is yes, this possible violation will be treated as a “close call.” Otherwise, this possible violation will be treated as a “clear on its face” FFT candidate.

- A. Is there any disagreement amongst the audit team on whether the PV is a “clear on its face” or “close call” candidate: YES ☐ NO ☐
 - a. If yes, explain why:

[Click here to enter text.](#)

- B. Does this possible violation reveal a serious shortcoming in registered entity’s reliability-related processes (e.g. a systematic compliance program failure):

YES ☐ NO ☐

- a. If yes, explain why:

[Click here to enter text.](#)

- C. Are there any additional facts the audit team needs to know in order to comfortably designate this possible violation for FFT treatment: YES ☐ NO ☐

- a. If yes, state those facts:

[Click here to enter text.](#)

3. Did audit team inform registered entity that this possible violation qualifies for FFT treatment? YES ☐ NO ☐

- a. If so, on what date? [Enter Date.](#)

This item was submitted by [REDACTED] on 3/11/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-3a

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

R4.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

1/6/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 12/29/2015

Beginning Date of Possible Violation: 10/28/2015

End or Expected End Date of Possible Violation: 1/12/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-004-3a, [REDACTED] is obligated to minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by revoking access to Critical Cyber Assets within seven (7) calendar days for personnel who no longer require such access to Critical Cyber Assets.

A [REDACTED] contractor who had worked at [REDACTED] with NERC access to the [REDACTED] Physical Security Perimeter (PSP) ended their employment on October 28, 2015. On 12/29/2015 it was discovered that the former contractor's badge was still active in the [REDACTED] Physical Access Control System (PACS).

The badge was deactivated and screenshots are attached to this self-report as evidence that the badge is in a suspended state in PACS. A formal interview with the [REDACTED] Account Manager was conducted by [REDACTED]. Upon further review it was determined that the [REDACTED] Account Manager had never filled out the Contingent Worker HR [REDACTED] on October 28, 2015. It was not filled out until 12/28/2015.

When going to process the form, the name was spelled wrong and did not appear on the drop down so the manager incorrectly assumed that she was already off boarded. There is no confirmation email.

However, the [REDACTED] Account Manager did not follow one of the steps in the off-boarding procedure which instructed him to notify [REDACTED] Manager of the off-boarding, which could have prevented this Possible Violation.

It has been confirmed that the contractor's badge has been returned to [REDACTED] and they are no longer working at a [REDACTED] facility. [REDACTED] ran a report on 12/29/15 that

verifies the badge was not used to access to the [REDACTED] since 10/28/15.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

1. Badge was deactivated by [REDACTED] Badge shows suspended in PACS.
2. An Off boarding process/checklist was created and finalized for [REDACTED] in early January.
3. Badge has been recovered from contractor.
4. Account Manager was immediately coached when issue was discovered.
5. Additionally the Account Manager was also coached by his supervisor.

12/29/2015 – Badge was suspended.
12/29/2015 – Account Manager coached
1/5/2015 – Account Manager coached by [REDACTED] Supervisor
1/8/2016 – Off boarding process was created and finalized.
1/12/2016 – Badge was returned.

Provide details to prevent recurrence:

An off boarding procedure/process has been created and finalized. This will standardize the process between all regions.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

1/12/2016

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because the badge was not reclaimed or deactivated until 60 days after termination.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Power System is minimal because the badge was not used once the worker was terminated.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R4.

Applicable Sub Requirement(s): R4.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

1/6/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 12/28/2015

Beginning Date of Possible Violation: 12/1/2015

End or Expected End Date of Possible Violation: 12/23/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-004-3a, [REDACTED] is obligated to minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by revoking access to Critical Cyber Assets within seven (7) calendar days for personnel who no longer require such access to Critical Cyber Assets.

[REDACTED] has a policy that mandates a 30 calendar days break for contractors that have been on an assignment for 36 consecutive months. This break must occur even if the contractor will return and be placed on the same assignment when he or she returns to [REDACTED].

A contractor working in [REDACTED] who was on a [REDACTED] required 30 day furlough, still had NERC [REDACTED] ID badge access in the system for more than 7 days after going on furlough.

The manager knew the contractor was going on furlough and was sent an [REDACTED] to fill out to remove the contractor from the Human Resources system. The manager failed to fill out the [REDACTED] which triggers the removal of CIP access.

As a matter of course, another [REDACTED] group was making sure the contractors that should be on furlough were removed from the HR system. The group found this contractor still in the system and informed the responsible manager.

When the manager was contacted, he filled out the [REDACTED] to remove access, which occurred on 12/22/2015. He placed the termination effective date as of 12/1/2015. The request to remove access went to [REDACTED] who realized this was a Possible Violation of the CIP Standards since the contractor's access was not removed within seven (7) days of the termination effective date. [REDACTED] followed our internal process for reporting it.

also ran a report to determine whether the badge was used to obtain CIP physical access, which it was not. The contractor's CIP access was removed on 12/23/2015. The contractor had physical access to the [REDACTED] and [REDACTED].

At the time of this possible violation, the sites listed above had the following Critical BES Cyber Asset devices present;

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**



Are Mitigating Activities in progress or completed? ☒ Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

1. Badge was deactivated by [REDACTED]
2. Badge has been recovered from contractor.
3. Verbal interview was held with contractor by his or her manager as well as coaching as to what actions are not permissible once termination is effective.
4. Verbal interview was held with manager by upper management to review process of termination of contractor on a 30 day furlough/break.

A Root Cause Analysis (RCA) will be performed to determine why a request by the manager for removal of NERC CIP access was not submitted within the required compliance timeline. A mitigation plan will be developed and implemented to decrease the probability of this type of violation from reoccurring. Depending on the outcome of the RCA, we anticipate changes to policies and procedures and more thorough training of managers.

Provide details to prevent recurrence:

A Root Cause Analysis (RCA) will be performed to determine why a request by the manager for removal of NERC CIP access was not submitted within the required compliance timeline. A mitigation plan will be developed and implemented to decrease the probability of this type of violation from reoccurring. Depending on the outcome of the RCA, we anticipate changes to policies and procedures and more thorough training of managers.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

5/30/2016

Potential Impact to the Bulk Power System:

Actual Impact to the Bulk Power System:

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because badge was still active in the badging system for 23 days after the effective date of termination. [REDACTED] terminated access of the badge as soon as discovery was made.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Power System is minimal because no misoperations, emergencies or other adverse consequences to the Bulk Power System had happened as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 6/15/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-3a

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

7/21/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/16/2016

Beginning Date of Possible Violation: 2/16/2016

End or Expected End Date of Possible Violation: 2/16/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP 004 3 R4, [REDACTED] is obligated to provide NERC CIP physical access only as required.

On the morning of February 16th, 2016, a badging request for a one individual was submitted in [REDACTED] which involved NERC and Non NERC access. NERC and non NERC requests are supposed to be submitted separately to ensure they are processed without any issue. The following access changes were requested in that submission:

1. NERC access was requested to be removed from one site for the individual: [REDACTED] (NERC CIP Access)

2. Access was requested to be added for [REDACTED] non NERC sites for the individual: [REDACTED]

3. Two requests to alter information on non NERC accesses from what was previously provided: [REDACTED]

4. Three non NERC accesses were requested to be removed: [REDACTED]

Because the submission of CIP and non CIP access in the same access request causes issues, the request was rejected by a member of [REDACTED]

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

[REDACTED]

Provide details to prevent recurrence:

A root cause analysis is being performed to determine the best course of action to ensure this issue does not occur again. A completion date will be provided once the best mitigation steps are determined.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

3/17/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric System would be that an individual who was not approved for access would have access to a PSP and its BES Cyber Assets. If approached with malicious intent, this could affect the reliability of that specific site, but would be unlikely or limited in extent due to the other protections provided via the NERC CIP requirements and the training and supervision of the sites staff.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the Bulk Electric System was minimal. The access that was provided was never used and removed as soon as the error was discovered. The provisioning of access did not lead to any unauthorized access nor were any attempts to use that access made.

Additional Comments:

[REDACTED]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Previously Reported Regions:

Initial Mitigating Activities

Are Mitigating Activities In Progress?

Review Completion

Determination

Mitigation

Events

Documents

Related Violations

Related Violations

Scope Expansions

REGIONAL SCOPE EXPANSION ID		STATUS
30	4/20/2016	Scope Expansion Accepted

Summary

Date possible violation expansion was discovered:

Beginning date of new expansion of possible violation:

End or expected end date of new expansion of possible violation:

Detailed description and cause of possible violation:

Per CIP-004-3a 4.2, [REDACTED] is obligated to revoke such access to Critical Cyber Assets within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

A user's access to an operations center should have been removed on 1/5/16 after the 4th Quarter 2015 Manager's Quarterly Review. The user's manager performed the quarterly access review and determined the user no longer needed NERC and non-NERC access and submitted a request to have it removed. Due to the design of the [REDACTED] system – which does not process NERC and non-NERC requests on the same ticket – the user's access was not removed within 7 days as CIP-004-3a R4.2 requires.

Even with the [REDACTED] system limitations, there is a process that should have prevented this Possible Violation. A [REDACTED] worker reviews a daily report of the prior day's actions. On 1/6, she noticed the user's access had not been removed and asked the analyst that processed this ticket to go back and remove the access. The analyst designated to remove this access made a reminder to fulfill this request. After making the reminder, the analyst failed to remove the inappropriate access within 7 days. On 1/18/2016, the analyst discovered she had not removed the access, and promptly removed it.

The inappropriate access was to [REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed?

No

Date Mitigating Activities are expected to be completed:

7/29/2016

REGIONAL SCOPE EXPANSION ID

STATUS

Description of Mitigating Activities:

[REDACTED] is currently performing a Root Cause Analysis to determine the necessary Mitigating Activities to properly mitigate this issue to prevent recurrence of this issue. In particular, [REDACTED] will be focusing on properly implementing a new tool that will allow managers to directly remove their employees' access, preventing administrative mistakes like this in the future.

Details to Prevent Recurrence:

Successful completion of this Mitigation Plan will prevent or minimize the probability that [REDACTED] incurs further risk of alleged violations of the same or similar reliability standards requirements in the future because [REDACTED] will be coached through the utilization of a tool to improve human performance. Proper use of a self-check will minimize human performance errors going forward.

Actual Impact to the bulk power system:

Minimal

Initial Reliability Impact Statement:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Entity Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

Review**Review Date:**

4/20/2016

Reviewer:

[REDACTED]

Review Findings:

Accepted

Reviewer Notes or Comments:

Reviewed Scope Expansion

This item was submitted by [REDACTED] on 8/11/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-3a

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

R4.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

4/25/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: Yes

If yes, indicate which Region(s):

Date Reported to Region(s):

2/11/2014

Date Possible Violation was discovered: 4/12/2016

Beginning Date of Possible Violation: 4/3/2016

End or Expected End Date of Possible Violation: 4/13/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED] terminated employment voluntarily on 4/1/2016. The manager initiated the termination process on 3/21/2016 from [REDACTED] however, the record was saved as "draft" and not completed until 4/12/2016. The employees last work day was Friday, 4/1/2016, with an effective termination date of 4/2/2016.

Employee had NERC badge access to the [REDACTED]

The [REDACTED] was generated on 4/12/2016 at 12:30 pm. Based on this request, [REDACTED] removed the NERC badge access on 4/12/2016, although the badge itself was not deactivated until the badging system received the termination notice the following day.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The [REDACTED] was generated on 4/12/2016 at 12:30 pm. [REDACTED] disabled the NERC electronic access on 4/13/2016.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

Potential corrective actions being considered include:

Update onboarding and off-boarding tools to include more detailed instructions for NERC CIP access removals.

Improve manager training materials to include detailed CIP access removal training.

Start a periodic manager acknowledgement that signifies the manager understands the NERC CIP access removal procedures.

Adjust manager onboarding and off-boarding tools to allow managers to forward date terminations.

Perform a corrective action effectiveness review to determine the effectiveness of the corrective actions.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/13/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric is minimal since this was a normal termination and not a termination "for cause". The manager had collected the employee badge so physical access to a PSP was no longer possible. Potential NERC CIP electronic access was possible, however there has been no evidence to support such an event has occurred.

Provide detailed description of Actual Risk to Bulk Power System:

There have been no actual documented events associated with this potential violation or this individual.

Additional Comments:

Final Mitigating Activities and milestones will be determined when the Root Cause Analysis being performed by [REDACTED] has been completed.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/2/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R4.

Applicable Sub Requirement(s): R4.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

7/21/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/14/2016

Beginning Date of Possible Violation: 3/11/2016

End or Expected End Date of Possible Violation: 4/15/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Issue One: Date Possible Violation was discovered: 4/14/16 - Beginning Date of Possible Violation: 3/11/2016 - End or Expected End Date of Possible Violation: [REDACTED]

On April 4, 2016 [REDACTED] identified five separate occasions on the following dates, 3/1/2016, 3/10/2016 4/1/2016, 4/4/2016 where individuals transferred from their NERC relevant roles and did not have their access revoked within the time period required under CIP 004-3 R4.2. These were not terminations but transfers. The individuals had access to [REDACTED]

This was a result of a known issue in [REDACTED] tool that requires managers to select each role the users are a part of and from which they should be removed. The managers in each case did not understand that they had to remove the employee's business role as well as their technical roles. The technical role is the role in which the individuals had CIP access. As a result, the NERC access was not removed in seven days and the individuals inappropriately maintained NERC access between 4 and 37 days.

Employee 1

Request for access removal was placed on 3/1/2016

His access should have been revoked on 3/8/2016. His access was revoked on 4/14/2016.

He had unauthorized access for 37 days.

Employee 2

Request for access removal was placed on 03/10/2016

His access should have been revoked on 3/17/2016. His access was revoked on 4/14/2016.

He had unauthorized access for 28 days.

Employee 3
Request for access removal was placed on 4/1/2016
His access should have been revoked on 4/8/2016. His access was revoked on 4/15/2016.
He had unauthorized access for 7 days.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Employee 4
Request for access removal was placed on 4/1/2016
His access should have been revoked on 4/8/2016. His access was revoked on 4/15/2016.
He had unauthorized access for 7 days.

Employee 5
Request for access removal was placed on 4/4/2016
His access should have been revoked on 4/11/2016. His access was revoked on 4/15/2016.
He had unauthorized access for 4 days.


The PRAs and trainings were up to date for each of the individuals during the time the individuals maintained access. All five individuals did not use their access in [REDACTED] or [REDACTED] in the time frame which they inappropriately maintained access.

Applies to [REDACTED]
Issue Two: Date Possible Violation was discovered: 6/30/2016 - Beginning Date of Possible Violation: 2/1/2016 - End or Expected End Date of Possible Violation: 6/30/2016

After analyzing all variances, the following two (2) discrepancies were identified:
•Employee terminated: Manager termination notification not entered in the initiating HR system within 24 hours. One issue of this type was identified. Date of voluntary termination: 5/31/2016 Date of entry into initiating HR system = 6/9/2016.
•User transferred and access not removed in the business area system when requested. One issue of this type was identified. Date of transfer = 2/1/2016 Date of access removal 7/1/2016.

Each of the above items represents a violation of CIP-004-3 R4.2. Through an extent of condition, each business unit will need to determine which, if any, discrepancy is a reportable potential violation. Any additional potential violations will be added to this self report.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Issue One: The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:
[REDACTED] implemented a technical solution to [REDACTED] that prevents managers from submitting a request for NERC access revocation without selecting the appropriate CIP permissions.

Issue Two: The mitigating activities [REDACTED] plans to undertake are as follows:
-All open discrepancies have been researched as of 6/30/2016.

Provide details to prevent recurrence:

Issue One: The actions that [REDACTED] is taking to prevent recurrence include the following:: Immediate corrective action of revoking NERC CIP access, the use of a new tool called [REDACTED]. The technical solution previously detailed will prevent recurrence of this issue. In addition, [REDACTED] will be performing a cause analysis and mitigation plan to correct any issues identified in the cause analysis.

Issue Two: To prevent further recurrence, a thorough analysis of the identified discrepancies was conducted and a review of the established roles was performed. A root cause analysis will be performed. Detailed findings will be identified and incorporated in the mitigation plan. Date Mitigating Activities are expected to be completed: 11/30/2016

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/15/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Issue One: The Potential Impact to the Bulk Power System is minimal because the access was revoked as soon as it was discovered on 4/14/2016. All non-mandatory access has been revoked for the users.

Issue Two: The potential impact to the Bulk Power System is minimal because web access for terminated employees is immediately revoked. The remaining employees received appropriate NERC CIP training, Personnel Risk Assessment and is knowledgeable of NERC CIP procedure.

As part of the extent of condition for this alleged violation, all business areas conducted second quarter access reviews; no issues were identified.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Actual Risk to Bulk Power System:

Issue One: There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation as these individuals never used their access during the time period in which it should have been revoked.

Issue Two: There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/12/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R5.

Applicable Sub Requirement(s):

5.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 5/3/2017

Beginning Date of Possible Violation: 4/13/2017

End or Expected End Date of Possible Violation: 4/13/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

A contractor with NERC physical access had his access terminated outside of the 24 hour requirement after leaving his contract company.

On April 13, 2017 the [REDACTED] performed a review of all NERC CIP badged individuals in his region and identified the contractor as no longer requiring unescorted access. Additionally, the [REDACTED] identified the contractor had changed employers; further investigation indicated the change occurred on July 15, 2015. Both employers performed work for [REDACTED] in the [REDACTED]. The 1st employer did not notify [REDACTED] of the contractor's departure in July 2015. The [REDACTED] directed the [REDACTED] to immediately revoke NERC access for the contractor, which was completed on April 13, 2017.

This potential violation was discovered on May 3, 2017 during review of the late termination entry report for the month of April 2017.

The contractor had physical access to the following sites:

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken with respect to this issue include:

- All NERC badged contractors in the [REDACTED] with physical access were reviewed and the need for continued NERC access to PSPs was validated.
- Notification letters were sent to all contractor companies supporting [REDACTED] teams reiterating the contractual requirements to notify [REDACTED] within 24 hours of any employment status change for NERC badged contractors.
- Contractor companies were required to sign and return acknowledgements of the contract requirements for notification within 24 hours.

Provide details to prevent recurrence:

- NERC badged [REDACTED] employee and contractor lists are reviewed monthly by the [REDACTED] team to validate all badged individuals still have a business need for access.
- Monthly validation with contractor companies to confirm employment status of NERC badged individuals is ongoing.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

9/22/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric System (BES) is minimal because the individual maintained required training, had an active PRA, had a business purpose for access to the NERC CIP Assets and continued to perform work for [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

No actual impact to the Bulk Electric System was caused by this possible violation because no unauthorized access attempts were made to the NERC CIP Assets. As a result, no emergencies, or other adverse consequences to the Bulk Electric System occurred due to this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 12

Record documents for the violation of CIP-004-6 R4

12.a The Companies' Self-Report

12.b The Companies' Self-Report

12.c The Companies' Self-Report

12.d The Companies' Self-Report

12.e The Companies' Self-Report

12.f The Companies' Self-Report

12.g The Companies' Self-Report

This item was submitted by [REDACTED] on 2/28/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-004-6

Applicable Requirement: [REDACTED]

R4.

Applicable Sub Requirement(s): [REDACTED]

4.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

10/11/2013

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Report

Has the scope of the Possible Violation expanded: [REDACTED]

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

9/23/2016

Beginning Date of Possible Violation: [REDACTED]

9/23/2016

End or Expected End Date of Possible Violation: [REDACTED]

9/23/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 9/14/2016, the [REDACTED] team received an approved request to add NERC badge access for an individual to multiple NERC CIP PSPs. Access provisioning started as requested on 9/20/2016 at approximately 10 AM. In the process of provisioning access, the work item was not marked completed and closed. The member of [REDACTED] was waiting for the last process step to complete before closing the work item that was to validate access in the [REDACTED] PACS System which had not yet occurred. The analyst handling the addition returned to her other work and neglected to return to the work item and close it once the verification had completed.

On 9/20/2016, at approximately 1:20 PM, a second approved request was received to remove a portion of the NERC badge access for the same individual. That removal of access was processed at 3:20 pm that same day.

On 9/23/2016, at approximately 10:25 AM, the original work item was revisited by a different analyst. That analyst checked the access, saw that it was not present, and re-processed the work item. That resulted in adding the access back that was removed in the second request. Notification was emailed to the individual's supervisor on 9/23/2016 at 1:37 PM. The supervisor contacted a [REDACTED] lead analyst to have the access corrected. The [REDACTED] lead analyst corrected the access and verified in [REDACTED] that as of 9/23/2016 at 2:34 PM, the individual who was provided access no longer had access to the following sites:

[REDACTED]

Overall, the improper access was in place for approximately 70 minutes (from 1:37 PM on 9/23/2016 to 2:47 PM that same day). This user was not used during that time. We have instituted additional manual checks for like-scenarios where there are multiple requests for the same person. Additionally, a stand down was held to bring awareness to and discuss the situation and what steps need to be implemented to prevent a reoccurrence.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

There is minimal impact to the Bulk Power System. The user access was modified in error and the user was unaware that they had been given additional privileges. The short amount of time that the user had the inaccurate access would not have allowed her time to enter the additional locations due the sites being located in different states.

validates PRA and Training at the time of the access request. It does not allow the access request to be submitted if the worker doesn't have the required training and PRA for the roles being requested.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation. During the 70 minutes that the non-required access was provided, it was not used.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 6/19/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

4.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

2/28/2017

Monitoring Method for previously reported or discovered:

Self-Certification

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/26/2017

Beginning Date of Possible Violation: 3/23/2017

End or Expected End Date of Possible Violation: 7/21/2017

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]
On 3/20/2017 an [REDACTED] started the transfer of files from the folder [REDACTED] to the [REDACTED]

During this process, the [REDACTED] noticed that the files/data being transferred was creating a performance issue on the [REDACTED] due to the large amount of data attempting to be transferred. On 3/23/2017, a work order [REDACTED] was submitted by the [REDACTED] to have the files that were moved during the transfer restored back to the server [REDACTED]. This server is a [REDACTED] device which uses [REDACTED]

When using shadow copy, the permissions of the folder [REDACTED] inherit the same permissions as the parent folder. As a result, the new permissions from the parent folder provided additional personnel access to the [REDACTED] device.

After a review of the personnel with this access, it was determined that some personnel inherited unauthorized permissions. The ticket [REDACTED] was created on May 18, 2017 to restore the old permissions and was completed on May 18, 2017. Access was granted to historical compliance data. This data will be retired as part of the repository cleanup effort which is expected to be completed by September 30, 2017.

A cause analysis will take place to assist in preventing recurrence of this possible violation on NERC CIP repositories.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal, due to the users having access to historical data that is [REDACTED] and does not reflect the current state of NERC CIP compliance within [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/8/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-6

Applicable Requirement: R4.

Applicable Sub Requirement(s): 4.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 3/30/2017

Beginning Date of Possible Violation: 2/27/2017

End or Expected End Date of Possible Violation: 10/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

On 02/27/2017 and 02/28/2017

[REDACTED] were performing [REDACTED] tuning with the assistance from a [REDACTED] vendor. The [REDACTED] vendor used a [REDACTED] Engineer's keyboard and mouse to navigate through various displays to instruct the [REDACTED] personnel on new functionality features for tuning [REDACTED] on the recently upgraded [REDACTED] platform version [REDACTED]. The vendor entered data into the [REDACTED] for certain parameters while tuning [REDACTED]. At no time did the vendor have unsupervised access to the [REDACTED] however, the vendor was not authorized to have electronic access to the [REDACTED] per the [REDACTED] process for compliance with CIP-004-6 R4 (Appendix 1). Unauthorized electronic access to the [REDACTED] could result in accidental or intentional actions performed on the BES which could compromise its integrity.

An Apparent Cause Analysis (ACA) was performed and the following causes were identified:

- Cause 1: Authorized ESP access for the [REDACTED] Vendor was not pursued by [REDACTED] management. This decision was made based on the relatively short length of time the vendor would be on-site, even though work on the [REDACTED] was expected and which requires authorized ESP access.
- Cause 2: [REDACTED] personnel performing the work with the [REDACTED] vendor did not question whether authorized ESP access was needed or had been granted. There was a general misunderstanding that "escorted" ESP access was authorized.

Initial mitigating actions taken:

- The [REDACTED] vendor was immediately prohibited from continued access to the [REDACTED] system.
- A review of CIP Standard CIP-004-6, R4 with direct reports in [REDACTED] that visitors that have not been granted electronic access shall not manipulate the mouse and keyboard on any CIP BES Cyber System.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the BES could have been moderate if the [REDACTED] Vendor was unknown to the [REDACTED] personnel in the control center and had been left in an unattended state to perform this work.

Provide detailed description of Actual Risk to Bulk Power System:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

There was no actual impact to the BES caused by this possible violation because the [REDACTED] vendor (a) had previously completed a personnel risk assessment and required training for their participation in the original system implementation and (b) was continuously monitored while access the system by several [REDACTED] personal in a training capacity. As a result, there were no misoperations, emergencies, or other adverse consequences to the BES.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 11/27/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-004-6

Applicable Requirement: [REDACTED]

R4.

Applicable Sub Requirement(s): [REDACTED]

4.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/11/2017

Beginning Date of Possible Violation: 2/26/2017

End or Expected End Date of Possible Violation: 8/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED] documented processes and Procedures applicable to this issue under CIP-004-6:

[REDACTED] processes to authorize electronic access is contained in [REDACTED]

Job Aid: Request NERC CIP Access for a worker [REDACTED]

requires the employee's manager to submit a request in [REDACTED]

[REDACTED] can grant and revoke access in the end system when direct provisioning is [REDACTED]

When direct provisioning is not configured, the Job Aid: Update worker NERC CIP access [REDACTED] outlines the process used when an end system owner must manually provision access in the end system to match the request in [REDACTED]

Applicable Sections of the documented processes:

Summary of possible violation

While performing the quarterly access review for Q2, 2017, [REDACTED] discovered an access authorization discrepancy for a [REDACTED] Employee. The employee was granted access to a [REDACTED] password repository on the actual [REDACTED] site without being processed and authorized in the [REDACTED] access management tool. This access was granted sometime between April 10th and May 22nd of 2017. [REDACTED] has verified the access was properly authorized in the [REDACTED] system on July 12, 2017. As a result, there is a possible violation of the below referenced standard and requirement because there was no authorization record for this access in [REDACTED] between April 10, 2017 and July 12, 2017.

Timeline

November 10, 2015 – The [REDACTED] was created. [REDACTED] documents.

Two access groups were created for the [REDACTED] site. One admin group (write access), and one visitor group (read only access). Access to the visitor group was granted based on a list of employees assigned to a Business Unit ID. The Business Unit ID used was the [REDACTED] and included [REDACTED]. Therefore, read only access to the [REDACTED] site was granted or revoked automatically (updated daily) based on if an employee was assigned to the Human Resource (HR) Table for the [REDACTED]. The read only automated group was created based on a request from the [REDACTED] to grant everyone read only access that was assigned to the [REDACTED]

Note:

The

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

February 29, 2016 – The [REDACTED] was first used by [REDACTED] to manage Access Requests for NERC CIP Access Credentialing.

April 10, 2017 – [REDACTED] Employee start date with the company. (For clarity, this [REDACTED] Employee is shown with identifier [PV] throughout this report)

May 22, 2017 – [REDACTED] conducted Q2 Access Review and uploads the results to a Data Validation Tool. [REDACTED] receives the Q2 Access Review report and begins generating a discrepancy report to compare the access requests in [REDACTED] to the personnel access records.

June 6, 2017 – NERC CIP training for the [REDACTED] Employee[PV] required for access to the [REDACTED] was completed. Training requirements are completed to meet CIP-004 R2.1 and R2.2. All courses and the PRA are required for a person with both the tools to access (i.e. CIP Passwords) and the means to access (i.e. physical access inside the [REDACTED]) NERC CIP [REDACTED].

June 30, 2017 – [REDACTED] and the [REDACTED] review the discrepancy report, and determine there was no [REDACTED] request for access to the [REDACTED] for the [REDACTED] Employee[PV], but the [REDACTED] Employee[PV] had access to the [REDACTED]. This means at some point between April 10th and May 22nd the [REDACTED] Employee[PV] was granted access to the [REDACTED] without a request in [REDACTED].

July 11, 2017 – An access removal request was submitted for the [REDACTED] Employee[PV] by [REDACTED] using the [REDACTED]. Note: This request was not completed due to the access authorization requests submitted for the July 12th [REDACTED] system update.

July 12, 2017 – A request was submitted by the [REDACTED] Employee's[PV] Supervisor to a member of the [REDACTED] to add the [REDACTED] Employee[PV] to the [REDACTED]. Note: This access authorization request was part of a [REDACTED] system update and a batch of [REDACTED] Employees were approved for access at the same time as part of this system update.

August 11, 2017 – Access management for the [REDACTED] system update. Access management was moved to [REDACTED].

Causes of the violation

Apparent Cause #1 Human Errors or Inappropriate Actions, Inadequate Skills or Knowledge

Access Management to the [REDACTED] was automated from a link with Human Resources system for the read only access level. This automation added the [REDACTED] Employee[PV] without a request in [REDACTED]. The [REDACTED] owners [REDACTED] and [REDACTED] Site Administrators were unaware adding the automation functionality is not permitted by the [REDACTED].

Contributing Cause 1: Organizational & Programmatic Deficiencies, Organization to Program Interface Deficiencies,

There is no procedure stating the requirement that a request in [REDACTED] shall exist before a person can be granted access to the [REDACTED]. When the compliance group requested an access restricted location be created as a CIP Password repository for [REDACTED] the access management requirement was not documented in a procedure or process flow.

Contributing Cause 2: Organizational & Programmatic Deficiencies, Organizational Breakdowns

The requirement that a request in [REDACTED] shall exist before a person can be granted access to the [REDACTED] had not been communicated to the [REDACTED] or the [REDACTED]. If the [REDACTED] owners would have known they would have been able to communicate this to the [REDACTED] Admins before the automation was added. When the [REDACTED] site was created and the access automation was added to the read only group this requirement was not communicated to the [REDACTED] Administrators. Thus, the [REDACTED] site admins needed this information in order to make the necessary informed decision whether to add or not to add the automation based on the Human Resources System tables.

An Extent of Condition form was sent to all business areas and responses are attached to the Discovery Tab of the [REDACTED] Possible Violation record. The ACA Lead and [REDACTED] CIP Lead reviewed the EOC responses and added details in the table below. The quarterly NERC CIP access reviews used by the [REDACTED] did not discover additional employee with unauthorized access for any other system outside of the PVs listed below.

The two questions issued in the EOC form where,

- 1) Describe the controls your [REDACTED] has in place that would prevent the event described in this report?
- 2) Does your Business Area have [REDACTED] that have employees provisioned automatically based on HR Data Tables?

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, equipment failures or other events that caused an actual impact to the Bulk Power System as a result of this alleged violation.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 1/22/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R4.

Applicable Sub Requirement(s):

4.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 11/13/2017

Beginning Date of Possible Violation: 10/28/2017

End or Expected End Date of Possible Violation: 11/13/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]

During the Q3 quarterly access review on 11/13/2017, it was discovered that an analyst assigned a user to the default group [REDACTED]

[REDACTED] appliance; this occurred on 10/28/2016. The user should have been assigned to the [REDACTED]

The reason this error was not addressed in the previous quarterly access reviews was because the discrepancy was believed to be a typo. When the error appeared again in the third quarter, it was investigated and discovered to be an actual error.

Are Mitigating Activities in progress or completed? Yes

An Informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Provide details to prevent recurrence:

[REDACTED] has identified corrective actions and will implement the actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that [REDACTED] will incur further risk of the same or similar NERC requirements in the future.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

12/12/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal as the [REDACTED] The user also maintained valid NERC CIP training and a Personnel Risk Assessment (PRA). This represents a minimum risk to the Bulk Power System (BPS).

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]. In January 2017, [REDACTED] conducted a review of Electronic Access Control or Monitoring Systems (EACMS) used for authentication and/or authorization, where a "pool" of devices generally has equivalent ability to respond to authentication/authorization requests. This review was designed to ensure that, where identifies an IT cyber asset as an EACM, all of the equivalent devices are also correctly classified and protected.

The devices [REDACTED] reside in the [REDACTED] CS and the following number of devices are with this BCS:

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

– 74357 – Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
– 74363 – Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
– 74355 – Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 1/23/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

4/7/2017

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: Yes

If yes, indicate which Region(s):

Date Reported to Region(s):

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

[REDACTED] Servers and [REDACTED] Servers were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Method of Discovery

Self-Assessment:

Extent Of Condition:

As part of the [REDACTED] the [REDACTED] group will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with the [REDACTED] and 2) ensure [REDACTED] the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [REDACTED] requirements of the process, no process available.

Cause Identification:


- Prior self-reported issues with [REDACTED] and other firewall rules focused on systems designed to facilitate [REDACTED] were incorrectly implemented due to the lack of clarity in the [REDACTED]
- [REDACTED]
- [REDACTED] were not previously identified as EACMS because their primary function was not to enable remote access

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [REDACTED] requirements of the process; no process available.

Prior self-reported issues with [REDACTED] and other firewall rules, focused on systems designed to facilitate [REDACTED] and were incorrectly implemented due to the lack of clarity during the implementation of the [REDACTED] program.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

On 11/28/2017, [REDACTED] determined this violation a self-report and the [REDACTED] submitted the appropriate [REDACTED] ticket workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

Provide details to prevent recurrence:

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar NERC reliability standard violation. ██████████

PROVIDED AND NOT CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

██████████ to perform a gap analysis and re-evaluation of in-scope BES Cyber Assets

- With oversight from ██████████ all ██████████ to perform a business procedure / gap analysis between the current CIP-002 / ██████████ documentation and the updated CIP-002 / ██████████ documentation
- With oversight from ██████████ all ██████████ to provide a draft of CIP-002 / ██████████
- With oversight from ██████████ all ██████████ to obtain ██████████ approved
- With oversight from ██████████ all ██████████ to identify those individuals who require training on updated CIP-002 / ██████████
- With oversight from ██████████ all ██████████ to communicate and provide training on updated CIP-002 / ██████████ to those individuals requiring training
- With oversight from ██████████ all ██████████ to re-evaluate / re-classify BES Cyber Assets based on updated business level procedures and submit potential violation if identified
- ██████████ to submit ██████████ tickets to initiate workflow necessary to re-classify identified devices as EACMS
- ██████████ to perform an active review of All ██████████ to determine if any additional systems have been improperly classified
- ██████████ to submit ██████████ tickets to push firewall rules for scanning identified devices
- ██████████ to perform ██████████ on identified devices

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/28/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
-------	----------	-------------	---------------------

No data available in table

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Risk to the Bulk Electric System

From a BES impact standpoint this event is considered moderate because:

The mis-classification of BES Cyber Assets could lead to BES Cyber Assets not receiving full NERC CIP protection.

The consequences of this event are considered moderate since mis-classification of BES Cyber assets include the potential that the following controls have not been verified:

- 1) Network port & service identification
- 2) Vulnerability and wireless scanning

Baseline management including:

- 1) Operating system/firmware
- 2) Software version
- 3) Logical network accessible ports
- 4) Security patches
- 5) Malicious code prevention security event monitoring system access controls

Provide detailed description of Actual Risk to Bulk Power System:

██████████ did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

The likelihood that this event would adversely impact the Bulk Electric System is considered minimal because:

Additional Comments:

This violation was not the result of intentional action to violate a NERC reliability standard. ██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this potential violation. The ██████████ internal compliance plan was in effect at the time of the potential noncompliance. ██████████ management relevant to the situation actively participated and encouraged employees to provide complete information.

There have been no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section

Attachment 13

Record documents for the violation of CIP-004-6 R5

13.a The Companies' Self-Report [REDACTED]

13.b The Companies' Self-Report [REDACTED]

13.c The Companies' Self-Report [REDACTED]

13.d The Companies' Self-Report [REDACTED]

13.e The Companies' Self-Report [REDACTED]

13.f The Companies' Self-Report [REDACTED]

13.g The Companies' Self-Report [REDACTED]

13.h The Companies' Self-Report [REDACTED]

13.i The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 9/12/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R5.

Applicable Sub Requirement(s):

5.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/16/2017

Beginning Date of Possible Violation: 1/1/2017

End or Expected End Date of Possible Violation: 6/16/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies only to [REDACTED]

On June 16, 2017 eight contractors with NERC access to a physical security perimeter (PSP) had their access terminated outside of the 24 hour requirement.

On June 16, 2017 the [REDACTED] completed the 2nd Quarter NERC Access Review for his region. During this review he identified eight (8) contractors who no longer required access. The 8 contractors worked for three (3) separate contracting companies providing facilities maintenance services to [REDACTED]

In November 2017, [REDACTED] the Facilities Management service provider for [REDACTED] changed contractor companies providing services. Contract termination letters were sent to 3 contract companies, effective 12/31/2016. At the time of contract termination, the NERC badged contractors did not have their physical PSP access removed for the [REDACTED]. The contractors' access should have been revoked by January 1, 2017.

The potential violation was discovered on June 16, 2017 during the quarterly NERC Access Review. The NERC access for all 8 contractors was immediately revoked.

Site in scope:

Are Mitigating Activities in progress or completed? Yes

An Informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

- All NERC badged [REDACTED] contractors in all regions with NERC physical access were reviewed and the need for continued NERC access to PSPs was validated.
- Notification letters were sent to all contractor companies supporting [REDACTED] and Project Management teams reiterating the contractual requirements to notify [REDACTED] within 24 hours of any employment status change for NERC badged contractors.
- Contractor companies were required to sign and return acknowledgements of the contract requirements for notification within 24 hours.

Provide details to prevent recurrence:

- NERC badged [REDACTED] employee and contractor lists are reviewed monthly by the [REDACTED] to validate all badged individuals still have a business need for access.
- Monthly validation with contractor companies to confirm employment status of NERC badged individuals is ongoing.
- Weekly reporting to [REDACTED] on NERC badging additions and removals is underway to maintain focus.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

9/22/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric System (BES) could be moderate given the duration of outstanding access and the fact the access was to high risk assets. Since this PSP is electronically and physically monitored 24x7x365, access was limited to physical access, and no unauthorized access attempts were made, it is concluded the potential risk is moderate.

Provide detailed description of Actual Risk to Bulk Power System:

No actual impact to the Bulk Electric System was caused by this possible violation because the NERC CIP BES Cyber Assets were not accessible by the individuals with late access revocation records. Additionally, no unauthorized physical access attempts were made. As a result, no emergencies, or other adverse consequences to the Bulk Electric System occurred due to this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/12/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 1/23/2017

Beginning Date of Possible Violation: 12/8/2016

End or Expected End Date of Possible Violation: 8/2/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

The SR applies to [REDACTED]
A co-op employee's last day worked was Dec. 6, 2016. The termination action entry did not occur in the HR system until Dec. 8, 2016.
Employee, with NERC CIP access, retiring on June 1, 2017 was not terminated in the HR system till June 21, 2017
The delayed entries were discovered while performing a monthly termination review designed to identify potential delays in CIP access revocation.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

NERC CIP Access personnel listings were provided to each of the [REDACTED] managers. The importance of timely access revocation was emphasized to all participants involved in the late access revocation.

Provide details to prevent recurrence:

Quarterly access reviews have been implemented to ensure managers/supervisors are keenly aware of the employees having NERC CIP access on their team.

2/3/2017

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate. The terminated employees had only physical access to five (5) PSPs at [REDACTED] all of which contained Medium Impact Cyber Systems, no High Impact Cyber Systems. [REDACTED]

Delayed access revocation creates a situation where the potential exists for unauthorized personnel to enter restricted areas, however in these 2 Self Reports, this risk was not realized. Both terminated employees were current in training and PRA requirements at the time of termination. In both instances, the badge was collected after it was deactivated. There were several alternate risk mitigation factors during these events. These alternative mitigation factors as well as the moderate risk associated with access revocation result in the overall potential risk to the Bulk Power System being moderate.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Electric System is minimal. There was no Actual Impact to the Bulk Power System caused by this potential violation because the terminated employees did not access the PSPs after their termination dates.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/6/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.3.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

1/5/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/14/2016

Beginning Date of Possible Violation: 7/8/2016

End or Expected End Date of Possible Violation: 7/14/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Applies to [REDACTED]
In accordance with CIP 004-6 R2 [REDACTED] shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities and require completion of the training at least once every 15 months.

On May 24, [REDACTED] sent notifications to the [REDACTED] point of contact for facilities contractors to notify him of the need for one of his contractors to renew training. Several messages were exchanged to schedule training for the contractors and accommodate individuals' availability (both renewals and new contractors who need training for first time NERC CIP access). Training sessions were offered on June 8, June 23 and June 27. The following series of events and communications occurred leading up to the violation:

June 23, 2016 - [REDACTED] point of contact communicated to [REDACTED] that the individual in question would no longer need CIP access on June 23, 2016.

June 28, 2016 - [REDACTED] directed the [REDACTED] to have the individual's manager take appropriate measures to revoke access. This would include removing access using [REDACTED]

On June 30, a revised training completion report was distributed. This report showed the individual still having access.

July 14, 2016 - [REDACTED] discovers the individual's training is expired and access has not been removed when it expired on July 8th, 2016.


July 14, [REDACTED] discovered the individual's training expiration date has passed (July 8). [REDACTED] is notified to revoke the individual's access and [REDACTED] revoked access the same day.

The violation is a result of the manager's failure to follow the steps to revoke the individual's CIP access before his training expired. This violation is in reference to just one individual.

The [REDACTED] at which this violation occurred was [REDACTED]
The user had access to all devices at this location. This facility contains the following systems and assets:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue includes an immediate response to the issue by revoking their access.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include performing a cause analysis to identify root causes and a mitigation plan designed to address the specific causes identified.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

7/14/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the access was revoked on 7/14/2016. Furthermore, this individual never used this NERC access during the time period in which it should have been revoked . All CIP access has been revoked for the individual.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation. Furthermore, this individual never used this NERC access during the time period in which it should have been revoked.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-004-6

Applicable Requirement:

R5.

Applicable Sub Requirement(s):

5.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 12/7/2016

Beginning Date of Possible Violation: 10/19/2016

End or Expected End Date of Possible Violation: 2/4/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 12/06/2016, there was request (#4382) created in [REDACTED] which contained "add access" item and a "remove access" item for the same worker. The [REDACTED] tool had not generated work items for the add and remove items within the request, due to a lack of approval for the "add access" item until 12/08/2016. This meant that the "remove access" item was not complete within the mandated 24 hour period. Once the add was approved on 12/08/2016, the [REDACTED] tool generated work items and both the REMOVE [REDACTED] and ADD (various) work items were completed promptly.

The manager was vigilant, monitoring the Remove request to completion. Vigilance allowed improvement opportunity to be prioritized over other enhancements, so [REDACTED] tool could be updated to handle Removes separately from Adds, since approval process is different.

Product Owner had already, prior to incident with the tool, requested that tool be enhanced to separate Add and Remove requests.

On 12/06/2016, at approximately 12:21 PM, the request was placed in the [REDACTED] tool. Upon receiving approvals on 12/08/2016, the work items (add and remove) were completed.

Both the access requests involved only one worker. The ADD access was for [REDACTED] and the Remove request was for [REDACTED].

Overall, the access that was meant to be removed within 24 hours was in place for an additional 22 hours (i.e. a total of approximately 46 hours). It has been verified that the improper access was not used during that time.

This was discovered on 12/07/2016, after the manager inquired why access had not been removed based on an access request with both an ADD and a Remove that was submitted on 12/06/2016.

An enhancement to the [REDACTED] tool will be made in May 2017 to no longer allow both addition and removal of access in the same request. In the event a Manager attempts to do so, the tool will display a message informing them that the 'Add' and 'Remove' portions must be submitted in separate requests.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The May 2017 code enhancement (target completion 5/30/2017), as described above, will prevent this issue in the future. Upon request, a Remove Work Item will be automatically generated, without dependency on any manual approval. Today, Remove Work Items are already monitored through a 24-hour per day, 7-day a week mitigation, the work item is not addressed by [REDACTED] each day, LAN access is terminated until the NERC CIP access removal has been addressed.

Provide details to prevent recurrence:

See description of Mitigation Activities in the previous section.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

5/31/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate because the excess access permissions which were in place would have allowed an unauthorized physical access to elements of the [REDACTED]. Using this access an individual could have harmed or damaged assets which could have led to an impact of the Bulk Electric System. The fact that the [REDACTED] is a continuously manned facility which is highly monitored keeps it from being severe since detection of malicious activities was highly likely.

Provide detailed description of Actual Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because the period of time for which unauthorized access was in place was short (22 hours extra) and there is no indication that the expanded access was attempted to be used during that timeframe.

The manager was vigilant, monitoring the Remove request to completion. Upon enquiry, the 'remove request' was investigated and the root cause found. Product Owner had already, prior to incident with the tool, requested that tool be enhanced to separate Add and Remove requests. There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation. During the additional hours that the access was in place, it was not used.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 8/3/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-004-6

Applicable Requirement: [REDACTED]

R5.

Applicable Sub Requirement(s): [REDACTED]

5.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

6/19/2017

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Certification

Has the scope of the Possible Violation expanded: [REDACTED]

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/7/2017

Beginning Date of Possible Violation: 3/7/2017

End or Expected End Date of Possible Violation: 7/12/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Per NERC CIP-004-6, Cyber Security – Access Revocation:

R5.3 [REDACTED] is obligated to ensure that individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic is revoked by the end of the next calendar day following the effective date of the termination action.

On 7/7/2017, during the review of the [REDACTED] it was discovered that access for seven workers was not removed from a [REDACTED] backup server [REDACTED] when access was removed from the [REDACTED] primary server [REDACTED]

On 2/29/2016, [REDACTED] established and implemented a base set of roles for workers per their defined access to various cyber or physical assets with NERC CIP impact.

The [REDACTED] compliance monitor for the [REDACTED] receives reports from the support teams on a quarterly basis. These reports detail who has access to [REDACTED] systems managed by [REDACTED]. The compliance monitor compiles these reports into a spreadsheet and loads into [REDACTED] which is used to validate access. The previous reports showed that the workers were removed from the [REDACTED] primary server [REDACTED] when required; however, their access was not removed from the [REDACTED] backup server [REDACTED]

In the previous quarterly reviews (2016 Q2, Q3, Q4 and 2017 Q1), the compliance monitor received information regarding the primary server but not the backup server.

Without the backup server information, the unauthorized access for the seven workers on the [REDACTED] backup server [REDACTED] was not discovered until the Q2 2017 review. This unauthorized access (7 users) was removed from the backup server as of July 12, 2017.

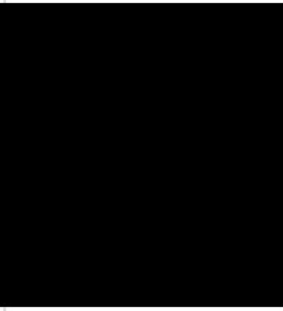
In order to help prevent reoccurrence:

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

During follow-up meetings with staff members, [REDACTED] Managers updated revocation procedures and provided clear instructions to include a review of both primary and backup devices/servers doing future removal of user access. This was completed as of July 21, 2017.

A cause analysis will be performed to identify additional actions required to prevent recurrence of this type of potential violation.

BES Cyber System and assets:



Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate, due to the fact that the workers continued to have access to a system that they no longer needed. [REDACTED]
[REDACTED] The workers involved continue to work for [REDACTED] and maintain the prerequisites to keep their NERC access.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 12/4/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-6

Applicable Requirement: R5.

Applicable Sub Requirement(s): 5.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/11/2017

Beginning Date of Possible Violation: 2/27/2017

End or Expected End Date of Possible Violation: 7/13/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

"This self-report applies to [REDACTED]"

Per CIP-004-6 R5.2 For reassignments or transfers, [REDACTED] is obligated to revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

[REDACTED] documented processes and Procedures applicable to this issue under CIP-004-6:

[REDACTED] procedure for the compliance monitor to perform a review of electronic and physical access every quarter is contained in [REDACTED]

[REDACTED] processes to authorize and revoke electronic access is contained in [REDACTED] dated September 2017

This process is executed by an application called [REDACTED]

When direct provisioning is not configured, the Job Aid: Update worker NERC CIP access [REDACTED] outlines the process used when an end system owner must manually provision (grant or revoke) access in the end system to match the request in [REDACTED]

Applicable Sections of the documented processes:

The Job Aid: Request NERC CIP Access for a worker was not followed by the owner manually provisioning access.

Summary

While performing the NERC CIP quarterly access review for [REDACTED] required in [REDACTED], [REDACTED] discovered an access revocation discrepancy for a [REDACTED] employee. The employee had access to a [REDACTED] password repository and during the manager's access review, it was determined the employee no longer needed access. The manager removed the employee from the appropriate business role in [REDACTED] on February 26, 2017, thus updating the access authorization record to de-authorize access. However, subsequent manual steps were not followed by the [REDACTED] to revoke access on the end system itself ([REDACTED]). [REDACTED] has verified the access was properly revoked on the end system on August 9, 2017. As a result, there is a possible violation of the below referenced standard and requirement between February 27, 2017 and August 9, 2017 because access was not removed on the end system.

Causes of the violation

Apparent Cause 1 (AC1): Human Errors or Inappropriate Actions, Misjudgment

[REDACTED] did not complete the request to remove [REDACTED] access within [REDACTED] days after the access revocation request was submitted. The [REDACTED] Request was closed out, but the proper manual steps to remove access in [REDACTED] were not performed correctly, specifically the [REDACTED] was not modified to remove access.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Contributing Cause 1 (CC1): Human Errors or Inappropriate Actions, Inadequate Skills or Knowledge

[REDACTED] did not receive adequate training on the requirements to complete access revocation tasks. Entitlement Owner had no knowledge of the manual steps required to complete access removal requests.

Contributing Cause 2 (CC2): Organizational & Programmatic Deficiencies.

Tracking tools did not provide timely backend checks to verify access revocation requests are completed successfully and in the required 24 hour timeframe

Contributing Cause 3 (CC3): Organizational & Programmatic Deficiencies.

CIP Quarterly access review procedural steps for discrepancies were not completed. All steps in Section 8.2 of the Quarterly Access Review Procedure were not completed to validate the removal task marked as completed by the role owner.

An Extent of Condition form was sent to all business areas [REDACTED] and responses are attached to the Discovery Tab of the [REDACTED] Possible Violation record. The [REDACTED] reviewed the EOC responses and added details in the table below.

The questions on the EOC form included:

- 1) [REDACTED] Do you have controls in place to ensure access granting or revocation are completed in the end system for each [REDACTED] request issued?
- 2) Describe how you know your control has prevented or will prevent the above situation.

The business areas listed in the NERC CIP EOC Group are, Representatives from [REDACTED]

The responses to the extent of condition stated that they use the [REDACTED] processes and procedures and do not have business area procedures or checklist to ensure manual steps are completed, when system automation is not used. No other Possible Violations related to this cause were identified when the extent of condition review was performed by other business areas outside of [REDACTED]

[REDACTED] for this Self-Report

The access was to a [REDACTED] site and no access to any BES Cyber System is possible.

Are Mitigating Activities in progress or completed?

Potential Impact to the Bulk Power System:

Actual Impact to the Bulk Power System:

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is Moderate. The employee no longer had a business need for the access and access was not revoked in the end system.

Provide detailed description of Actual Risk to Bulk Power System:

Verification was performed to ensure no actual access to the target systems. As a result, there was no Actual Impact to the Bulk Power System caused by this possible violation and there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 2/8/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-004-6

Applicable Requirement: [REDACTED]

R4.

Applicable Sub Requirement(s): [REDACTED]

4.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 9/27/2017

Beginning Date of Possible Violation: 8/22/2017

End or Expected End Date of Possible Violation: 10/31/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-004-6 R4.2, [REDACTED] is required to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records. Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing the work function.

Problem Statement:

On 9/27/2017, while researching discrepancies from the 2017 3rd Quarter [REDACTED] Access Review, the system that enables [REDACTED] to centrally manage access to Bulk Electric System (BES) cyber assets through business roles and access reviews, a [REDACTED] Analyst determined that [REDACTED] individuals were included in [REDACTED] Domain groups but did not have the appropriate business role to support being in the [REDACTED] groups.

Method Of Discovery:

Self-Assessment: [REDACTED]

Employee [REDACTED]

On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]

On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

On 12/14/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]

On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Employee [REDACTED]
On 7/6/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 7/6/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 6/1/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]


Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] Server Admins entitlement was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Employee [REDACTED]
On 2/27/2016, access to the Business Role [REDACTED] was approved and loaded into [REDACTED]
On 8/22/2017, while performing the quarterly access review, the manager requested employee be removed from this role
On 10/3/2017, the manager requested access be removed from the [REDACTED]

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

- A manual [REDACTED] ticket was submitted and executed to remove the individuals from the identified [REDACTED] Completed 9/29/2017
- As part of the Extent Of Condition (see Conclusion of the 2017 4th quarter [REDACTED] Access review), [REDACTED] verified that all "corrective ACLs" identified during the 2017 Q4 [REDACTED] Access Review, were uploaded into [REDACTED] and the associated Business Roles assigned appropriately. Completed 1/11/2018

Provide details to prevent recurrence:

[REDACTED] has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that [REDACTED] will incur further risk of the same or similar NERC requirements in the future.

- 1) [REDACTED] to update the quarterly access review process to include a validation and verification that all corrective Access Control Lists (ACLs), identified as part of a quarterly access review, have been uploaded into [REDACTED] and remediated the identified issue
- 2) [REDACTED] to review and update the quarterly access review process to a) Identify of all "disconnected" entitlements, b) Verification and validation that all corrective ACLs, identified as part of a quarterly access review, have been uploaded into the [REDACTED] c) Verification that a single corrective ACL is loaded into the [REDACTED] before the next corrective ACL is loaded or verification that all corrective ACLs, identified during the quarterly access review, are included in one ACL file, d) Identification of all system reports used to perform a quarterly access review, e) Methodology for using identified system reports to ensure all accounts are included on the quarterly access review, f) Human Performance tools such as "Peer Review" or "Peer Check" into the quarterly access review process
- 3) Implement Human Performance tools such as "Peer Review" or "Peer Check" into the quarterly access review process
- 4) Identify and perform training to individuals on updated processes
- 5) [REDACTED] to submit the appropriate access requests to remove those users identified during the 2017 Q4 review who do not have authorized access to identified entitlements
- 6) [REDACTED] to enhance the [REDACTED] to include information on user entitlements

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

9/29/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Potential Risk to Bulk Power System:

While [REDACTED] is implementing this mitigation plan it has identified minimal risk to the reliability of the Bulk Electric System (BES).

From a BES impact standpoint this event is considered minimal because:

- 1) All individuals that were in the [REDACTED] groups were approved to have the associated business role required to perform their job function prior to the role being removed
- 2) All individuals, that were in the [REDACTED] groups, remain NERC CIP-trained and have valid Personnel Risk Assessments (PRAs)

There is a minimal likelihood that this potential violation would be exploited. All individuals identified in this potential violation remain in a NERC CIP role and their NERC CIP training and background screening is current.

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because all individuals identified in this potential violation remain in a NERC CIP role and their NERC CIP training and background screening is current.

Additional Comments:

Facts, Evidence and Supporting Information:

- Not all NERC CIP [REDACTED] are electronically "connected" between [REDACTED] and [REDACTED] or the source system
- NERC CIP "systems" that do not use a direct interface with [REDACTED] are considered "disconnected" entitlements
- "Disconnected" [REDACTED] do not receive automatic updates in [REDACTED] when a change is made to the [REDACTED] or source system
- [REDACTED]
- To perform a quarterly [REDACTED] "disconnected" entitlements have to be manually added into an ACL spreadsheet and imported into the [REDACTED]
- The quarterly access review is a validation that only authorized users have been granted electronic access to BES Cyber Systems, BES CSI Repositories, and physical access to BES Cyber Assets
- The quarterly access review is achieved by comparing individuals' actual provisioned BES Cyber Systems, BES CSI Repositories, and physical access to BES Cyber Assets ACL against records of individuals authorized in [REDACTED] to the BES Cyber Systems, BES CSI Repositories, and physical access to BES Cyber Assets
- Any discrepancies identified between the actual provisioned access and the individual's authorized access are reviewed to determine the cause
- An individual that has an "additional entitlement" is an indication that the individual was included in the ACL but [REDACTED] does not have a record of that individual's authorized access
- An individual that has a "missing entitlement" is an indication that the individual was not included in the ACL but [REDACTED] has a record of that individual's authorized access
- When the 2017 Q2 validation was performed it was determined that individuals in [REDACTED] had "missing entitlements"
- To resolve the "missing entitlement" discrepancy, the Compliance Monitor should load a "corrective ACL" into [REDACTED]
- The [REDACTED] failed to load a "corrective ACL" for the identified [REDACTED] within the timeframe outlined in the quarterly access review process
- Prior to the 2017 Q3 quarterly access review, the manager for the identified individuals removed the [REDACTED] Technical Role from the identified individuals because their job no longer required that role
- When the 2017 Q3 ACL was created, the disconnected [REDACTED] identified in this potential violation were included in the 2017 Q3 ACL
- When the 2017 Q3 validation was performed, it was determined that the individuals now had "additional entitlements" because the [REDACTED] Technical role was removed from those individuals; however, the individuals were not removed from the [REDACTED] causing this potential violation
- Had a "corrective ACL" been loaded into [REDACTED] in a timely manner, when the manager removed the Technical Role from the respective individuals, [REDACTED] would have issued an automated work item to have the individual removed from the respective [REDACTED]

Human Performance / Inappropriate Actions:

- A complete ACL was not submitted prior to beginning the 2017 Q1 or 2017 Q2 [REDACTED] Quarterly Access Review
- A corrective ACL was not submitted after the 2017 Q1 or Q2 access review, as specified in the [REDACTED] Quarterly Access Review Procedure, section 9.1, to resolve missing entitlements

Procedure Use and Adherence Investigation:

- Less than adequate process to validate a complete ACL is submitted at the onset of a quarterly access review
- Less than adequate process for performing Quarterly Access Reviews and resolving identified discrepancies
- Less than adequate process to validate all corrective ACLs are loaded in the [REDACTED] to resolve identified discrepancies

Organizational / Programmatic Investigation:

- An Organization / Programmatic investigation was performed. No failures were identified

Equipment Failure Investigation:

- Although no equipment failures were identified during this cause analysis, the design of the [REDACTED] tool requires a substantial amount of manual processing to ensure the tool operates as designed. These manual processes are not sustainable and can lead to additional failures.

An extent of condition was performed to:

- 1) Verify all 2017 3rd quarter [REDACTED] Access reviews, for all [REDACTED] was performed
- 2) Where a manual [REDACTED] Work item should have been generated, determine if all access was removed for those individuals identified

On 12/2/2017, Senior Compliance Analyst [REDACTED] notified [REDACTED] that additional discrepancies were identified during the 2017 Q4 [REDACTED] Access Review. The results of the 2017 Q4 [REDACTED] Access Review will be completed by December 31, 2017 and any additional findings will be included in this cause analysis.

Conclusion of the 2017 3rd quarter [REDACTED] Access Review:

As part of each quarterly [REDACTED] Access Review, and for each [REDACTED] reviews the discrepancies that are identified through the Data Validation process. [REDACTED] determines if a discrepancy is the result of an "additional entitlement" or a "missing entitlement." In the case of an additional entitlement [REDACTED] works with the [REDACTED] to determine if the entitlement was missing from the uploaded ACL and if the discrepancy can be fixed by submitting a "corrective ACL" or if a Business Role was removed for the individual(s) and there is a possibility of a potential violation.

In the case of a missing entitlement, [REDACTED] works with the [REDACTED] to determine why the entitlement is not in [REDACTED] but was included in the uploaded ACL.

In the event a "corrective ACL" is required to resolve a discrepancy, [REDACTED] contacts the appropriate [REDACTED] to request the "corrective ACL" be loaded into [REDACTED]

Because this process is labor intensive for both [REDACTED] and the [REDACTED] Compliance Monitors, there is a possibility that all discrepancies are not remediated in a timely manner or the [REDACTED] does not submit the "corrective ACL" to address a discrepancy.

[REDACTED] has completed a review of the 2017 Q3 [REDACTED] Access Review and has determined no additional discrepancies were identified. [REDACTED] manual [REDACTED] work item should have been generated and access was not removed for the identified individuals.

UNCLASSIFIED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

The 2017 Q3 [REDACTED] Access Review was the first quarterly review that included BES CSI data. This specific failure will not be determined until the 2017 Q4 [REDACTED] Access Review is performed.

Conclusion of the 2017 4th quarter [REDACTED] Access review:

CIP Compliance Assurance completed the 2017 Q4 [REDACTED] Access Review, following the same process outlined above, and identified nine (9) individuals who were included in 3 [REDACTED] Entitlements but did not have the appropriate business role to support being in the respective entitlement.

In all instances, the ACL did not include the respective entitlement prior to performing the quarterly review. When the discrepancy was identified, as part of the respective quarterly review, there was a failure to load a corrective ACL into [REDACTED]. When the 2017 Q4 [REDACTED] Access Review was performed, the ACL included the entitlements in question; however, the respective manager had requested the business role be removed for the individuals identified.

[REDACTED] is submitting the appropriate access request forms to have the identified users removed from the identified entitlements.

In addition, [REDACTED] verified that all "corrective ACLs" identified during the 2017 Q4 [REDACTED] Access Review were uploaded into [REDACTED] and the associated Business Roles assigned appropriately. Completed 1/11/2018

The individuals identified during the 2017 Q4 [REDACTED] Access Review all remain in a NERC CIP function and their background screening and NERC CIP Training is up-to-date.

Cause Analysis

This violation occurred as a result of a less than adequate manual process for submitting a complete ACL at the onset of the quarterly access review, and subsequent corrective ACLs, to resolve any discrepancies that are identified during the quarterly access review, into [REDACTED]

In addition, the current process does not include Human Performance tools, such as "Peer Review" or "Peer Check," to ensure all identified "corrective ACLs" are submitted in a timely fashion to resolve any discrepancies that are identified during the quarterly access review.

Cause Identification

The [REDACTED] Quarterly Access Review Procedure does not ensure that the quarterly access review ACL includes all disconnected entitlements and subsequent corrective ACLs are submitted in a timely manner to resolve identified discrepancies as part of the quarterly access remediation.

The direct and contributing causes of this possible violation are as follows:

A less than adequate process is used during the [REDACTED] Quarterly Access Review to ensure the Quarterly Access Review ACL is complete and subsequent corrective ACLs are submitted to reconcile the differences identified between an individual's actual provisioned access to a BES Cyber System ACL, and the individual's authorized access to the BES Cyber System [REDACTED]

- Apparent Cause 1 (AC1): Less than adequate validation and verification of the scope of disconnected entitlements, that the Compliance Monitor is responsible for managing, for the initial quarterly ACL load caused the original discrepancy
- Contributing Cause 1 (CC1): Less than adequate validation and verification that all corrective ACLs are submitted into [REDACTED] to resolve identified discrepancies
- Contributing Cause 2 (CC2): Human Performance. The current Quarterly Access Review Procedure does not include Human Performance tools, such as "Peer Review" or "Peer Check," to ensure all identified corrective ACLs are submitted correctly and in a timely fashion

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-002-5.1

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 1/5/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 1/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]. In January 2017, [REDACTED] conducted a review of Electronic Access Control or Monitoring Systems (EACMS) used for authentication and/or authorization, where a "pool" of devices generally has equivalent ability to respond to authentication/authorization requests. This review was designed to ensure that, where [REDACTED] identifies an IT cyber asset as an EACMS, all of the equivalent devices are also correctly classified and protected.

This review identified that the [REDACTED] Domain, which can be used to log into devices that are in NERC CIP scope, had [REDACTED] servers that were not identified as EACMS. Based on the locations of these devices, they have performed EACMS functions for assets that are currently in NERC CIP scope and therefore should have been identified as EACMS. Device names are as follows:

The devices [REDACTED] reside in the [REDACTED] and the following number of devices are with this BCS:

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Yes, these devices were reclassified as follows:

- a. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- b. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17
- c. Mast ticket for CCA assessment. And was reclassified as a EACM on 1/10/17

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

A cause analysis will be performed to evaluate additional causal factors to identify effective corrective actions to prevent reoccurrence.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

1/11/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System was minimal. The devices reside physically within existing Physical Security Perimeters. User access to the is shared across all so existing access controls for domain users and administrators were enforced. User provisioning in the domain follows NERC CIP administration best practices, and the user population is limited to only personnel. Further, the reside behind Firewalls in DMZ networks. Finally, the suite of tools and best practices were used when the systems were commissioned, settings like Group Policy, Auditing, and Logging would have been in place from the initial build of the server. Based on these security measures that were in place, there was minimal likelihood that the failure to identify these devices as EACMS resulted in unauthorized or unauthenticated activity that could adversely affect the Bulk Power System.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED]

on 1/23/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-002-5.1a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

4/7/2017

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: Yes

If yes, indicate which Region(s): [REDACTED]

Date Reported to Region(s):

4/7/2017

Date Possible Violation was discovered: 11/15/2017

Beginning Date of Possible Violation: 11/15/2017

End or Expected End Date of Possible Violation: 11/17/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP002-5, R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

Per sub-requirement R1.1:

Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.

Problem Statement

Seven [REDACTED] and two [REDACTED] were not properly classified as High Impact Electronic Access Control or Monitoring Systems (EACMS), causing the devices to potentially not have full North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), resulting in this possible violation.

Additional Information:

Categorization of Bulk Electric System (BES) Cyber Assets (CAs), BCAs, is the process whereby a CA and then assigns the appropriate categorization to that device. Proper categorization of EACMS ensures appropriate NERC CIP protections are implemented on the identified asset.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Method of Discovery

Self-Assessment:

As a step in the build process for a net new server to support a net new instance of the [REDACTED] the [REDACTED] conducted the categorization review of this new server. During this review on 11/15/2017, he consulted with the [REDACTED] regarding the uses of this server. The [REDACTED]

During the categorization review conducted between the [REDACTED] as the first step in building a new [REDACTED]

While discussing functionality the [REDACTED]

After more discussion with a [REDACTED] it was determined that the [REDACTED] should also be categorized as EACMS.

Extent Of Condition:

As part of the [REDACTED] the [REDACTED] will provide additional guidance around the types of systems that constitute "Intermediate Systems." As a result of this guidance all [REDACTED] will need to 1) reassess their technologies to ensure alignment with the [REDACTED] and 2) ensure [REDACTED] processes support the new program which may require the [REDACTED] to work through the asset classification process for all assets under the revised program.

Cause Analysis:

This violation occurred as a result of:

- Lack of specificity within the [REDACTED] requirements of the process, no process available.

Cause Identification:


- Prior self-reported issues with [REDACTED] focused on systems designed to facilitate [REDACTED] were incorrectly implemented due to the lack of clarity in the [REDACTED]
- [REDACTED] were not properly assessed in the V5 transition as being Intermediate Systems
- [REDACTED] were not previously identified as EACMS because [REDACTED]

The direct and contributing causes of this possible violation:

Apparent Cause 1 (AC1): Process Weakness. Lack of specificity within the [REDACTED] requirements of the process; no process available.

Prior self-reported issues with [REDACTED] and were incorrectly implemented due to the lack of clarity during the implementation of the [REDACTED]

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

On 11/28/2017, [REDACTED] determined this violation a self-report and the [REDACTED] submitted the appropriate [REDACTED] workflow to correctly update the categorization and create the necessary work orders to apply the appropriate controls to the identified devices.

Completed: As of 12/4/2017, all identified devices have been re-categorized as EACMS.

██████████ has identified the following corrective actions and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that ██████████ will incur further risk of the same or similar PRAWNERC and/or CONFIDENTIAL IN

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

- 11/28/2017

Title	Due Date	Description	Prevents Recurrence
No data available in table			

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section

Attachment 14

Record documents for the violation of CIP-005-3a R1

14.a The Companies' Self-Report [REDACTED]

14.b The Companies' Self-Report [REDACTED]

14.c The Companies' Self-Report [REDACTED]

14.d The Companies' Self-Report [REDACTED]

14.e The Companies' Self-Report [REDACTED]

14.f The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 2/26/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-005-3a

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

R1.4.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

2/11/2015

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Report

Has the scope of the Possible Violation expanded: [REDACTED]

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/30/2015

Beginning Date of Possible Violation: 11/1/2014

End or Expected End Date of Possible Violation: 9/30/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Per CIP-005-3a, R1.4 requires that any non-critical cyber asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the standards in CIP-005-3.

Initially, in April 2013, there was a CVA walk down performed at the [REDACTED] and this device was discovered; however, it did not contain an Electronic Access Point (EAP) and was not added to the Critical Cyber Asset (CCA) list at that time; no additional actions were taken. Later, during a November 2014 walk down of the [REDACTED] in [REDACTED], the [REDACTED] switch was determined to be a cyber asset although it was not known at this time if the device was an in-scope NERC CIP asset.

The [REDACTED] was not included on the AIC list until June 30, 2015 when research on the device had been completed at this time and the device was determined to be a protected cyber asset (PCA).

On 4/30/2015, a baseline was created; however, the switch was not configured as a NERC CIP device and brought into full compliance until 9/30/2015. This was due to additional research being performed on the switch between 6/30/2015 and 9/30/2015 to validate that the PCA classification was, in fact, correct.

This asset is believed to have been in place before the [REDACTED] NERC CIP Compliance date; because we can't confirm the date, we are submitting it as a pre-NERC-CIP compliance asset.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Device was added to AIC list on 4/30/2015 as a PCA and configured as a PCA NERC-CIP asset on 9/30/2015.

Provide details to prevent recurrence:

██████████ procedures in support of V5 compliance are effective and being followed. Awareness communications will be prepared and distributed to appropriate management.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

3/30/2016

Potential Impact to the Bulk Power System: Severe

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Risk to the Bulk Power System is severe because in accordance with CIP-002-3 R3, all critical cyber assets/cyber assets must be identified, configured appropriately, approved and documented in order to appropriately protect the BES. Failure to identify the device means the appropriate protections were not in place for this device and inappropriate use of the device could have potentially occurred.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Device resided within secured and monitored PSPs that are monitored 24X7X365. The potential impact to the BPS is minimal because the other IT assets were provided all CIP security protection.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

██████████ was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-3a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.4.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

10/26/2012

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/11/2015

Beginning Date of Possible Violation: 1/27/2015

End or Expected End Date of Possible Violation: 2/13/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-005-3a R1.4, [REDACTED] is obligated to identify and protect any non-critical Cyber Asset within a defined Electronic Security Perimeter pursuant to the requirements of Standard CIP-005-3a.

While working through the Cyber Asset evaluation to move to CIP Version 5 it was discovered that the [REDACTED] at [REDACTED] was replaced with a [REDACTED] on 1/27/2015 and connected to the Electronic Security Perimeter (ESP). The original [REDACTED] was not previously connected to the ESP.

A review of the [REDACTED] compliance state was performed. It was determined two requirements in CIP-007-3a R5 and R6 are not meeting compliance.

R5)

R6)

The new [REDACTED] does not have automatic or manual alerts for detected Cyber Security Incidents enabled as required in CIP-007-3a R6.2. The device does have local logging enabled however there is no mechanism to report those logs/alerts automatically or through a process for a manual review.

There is only one device that is in scope for this Self-Report, the [REDACTED] No other Critical Assets have an [REDACTED] installed.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

1. Review documents required in CIP-007-3a.
2. Disconnect the [REDACTED] from the ESP.

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

1. Detailed Root Cause Analysis led by our Engineering Department to review all the project steps that need to be identified for CIP Compliance; Project Scoping, Design, Construction, and Commissioning.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

2/13/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the [REDACTED] The [REDACTED] was disconnected within three weeks from commissioning. All requirements for CIP-005 are met except for two under CIP-007-3a R5 and R6.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. There is only one device that is in scope for this Self-Report, the [REDACTED]. No other Critical Assets have an [REDACTED] installed.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 2/21/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-005-3a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.4.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 10/8/2015

Beginning Date of Possible Violation: 10/7/2015

End or Expected End Date of Possible Violation: 10/8/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-005-3a R1.4 [REDACTED] is obligated to have any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

On Wednesday October 7, 2015, around 3:15 pm, a Security Specialist arrived at the [REDACTED] for a 4pm meeting with various [REDACTED] employees. Prior to this meeting the Security Specialist found an empty office area where he could work on his company laptop and send out a few mails prior to the meeting.

Not finding a loose Network/LAN cable he removed the cable from the rear of PC [REDACTED] that was on the floor where he was working. When he disconnected the cable and put it into his corporate Laptop, he was not aware that this connection was inside the ESP secure network and proceeded to log into his Laptop and the network. It is my estimate that the LAN cable was connected into his laptop until 3:55pm, at that time he logged off his corporate computer and reconnected the LAN cable back into PC [REDACTED].

On the morning of October 8, 2015, he returned to the [REDACTED] around 8:30AM. On this day he returned to the same workstation that he disconnected the day before and removed the LAN cable from PC [REDACTED] and put it into his laptop in order to gain access to the network. He was connected for approximately four hours. At that time he reconnected the cable back into PC [REDACTED].

Around 4:30pm October 8, 2015, IT Security contacted the Security Specialist via email about his computer being connected into the ESP. The Security Specialist contacted IT Security via cell phone regarding their email. After talking to IT Security the Security Specialist contacted his manager about the incident.

There was only one Security Specialist involved in the incident and one CCA PC [REDACTED]

The incident was discovered due to [REDACTED] traffic on the network.

The [REDACTED] has the following systems and assets.

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following: The employee was talked too about the severity of the incident and their performance. The employee decided to resign from [REDACTED]

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following : All [REDACTED] personnel in [REDACTED] will be communicated about the importance of obeying the signage attached to equipment and requesting assistance if they need to utilize a CCA.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

10/12/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the BPSs minimal because connectivity was not allowed because of the firewall. The connected computer was blocked from connecting to the corporate network.

Provide detailed description of Actual Risk to Bulk Power System:

There was no actual impact to the BPS because the firewall blocked connectivity to the corporate network. [REDACTED]
[REDACTED] There were no mis-operations, emergencies or other adverse consequences to the BPS as a result of the alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 7/21/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-005-3a

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.5.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

4/13/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/1/2015

Beginning Date of Possible Violation: 12/31/2014

End or Expected End Date of Possible Violation: 8/31/2015

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This Self-Report applies to both [REDACTED] and [REDACTED]. The Applicable Functions for [REDACTED] are [REDACTED]. The Applicable Functions for [REDACTED] are [REDACTED].

Per CIP-005-3 R1.5, [REDACTED] is obligated to ensure all EACM devices adhere to the requirements in CIP007-3. CIP-007-3 R5.1.3 where at least annually the access privileges are reviewed to ensure they are correct.

[REDACTED] is in the process of implementing a new Identity Access Management tool that will assist in identifying critical cyber assets, accounts on those assets and the people who have access to those assets and accounts.

During discussions on the implementation of the new tool a question arose as to why EACM's (T2 & T4 critical assets) were not included in the 2014 CIP007-3 R5 Account Management review.

On April 1, 2015 the IT CIP Lead realized the [REDACTED] managed EACM's were not included in the CIP007-3 R5 Annual Account Management Review.

Below are the identified EACM's (Tier2 and Tier4) identified in the [REDACTED] region that were omitted from the Annual 2014 CIP007-3 R5 Account Management review.

[REDACTED]

Below are the identified EACM's (Tier2 and Tier4) identified in the [REDACTED] that were omitted from the Annual 2014 CIP007-3 R5 Account Management review.

and are located at the following sites:

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The EACM's have been identified and a review of the assets, applicable accounts and people who have access to those EACM's and accounts is in progress.

Provide details to prevent recurrence:

A process for identifying all assets to be included in the CIP007-3 R5 Account Management Annual review was implemented in a previous mitigation plan. The CIP Lead responsible for generating and implementing the account management review is aware of that process and will use that process for future CIP007-3 R5 Account Management reviews.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/31/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric System is minimal because the same individuals who have access to the identified EACM's also have access the Critical Cyber Assets that were included in the 2014 CIP007-3 R5 Access Management annual review and no unauthorized individuals were identified as having access to the Critical Cyber Assets in the 2014 CIP007-3 R5 Access Management annual review.

A review of the identified EACM's is currently underway and is anticipated to be completed by 8/31/2015.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

This item was submitted by [REDACTED] on [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-005-3a

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

R1.5.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 8/20/2015

End or Expected End Date of Possible Violation: [REDACTED]

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On [REDACTED] while working on an [REDACTED] audit data request, a logging anomaly was discovered and investigated. It was discovered that [REDACTED] had not been receiving logs for 1 [REDACTED] to syslog and then onto [REDACTED] where they could be monitored. [REDACTED] It was discovered that this was due to a hardware failure where a network card had stopped working and needed to be replaced. The [REDACTED] vendor was contacted and the network card/motherboard was replaced on 10/21/2015. [REDACTED] resumed receiving logs for the device on 10/21/2015 at 4:00 PM.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The faulty network card was replaced on 10/21/2015 and normal logging resumed in [REDACTED]

Provide details to prevent recurrence:

This issue occurred because of a hardware failure. This was due to the [REDACTED] device's failure to send the firewall logs to syslog and then onto [REDACTED] where they could be monitored. The issue has been resolved and mitigation steps to prevent recurrence are being investigated at this time.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

10/21/2015

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because any events that may have been logged were not able to be sent to the central logging and monitoring repository.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-005-3a

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.5.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 8/20/2015

End or Expected End Date of Possible Violation: 10/21/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On [REDACTED] while working on an [REDACTED] audit data request, a logging anomaly was discovered and investigated. It was discovered that [REDACTED] had not been receiving logs for 1 [REDACTED] firewall device since 8/20/2015. This was due to the [REDACTED] device's failure to send the firewall logs to syslog and then onto [REDACTED] where they could be monitored. [REDACTED] It was discovered that this was due to a hardware failure where a network card had stopped working and needed to be replaced. The [REDACTED] vendor was contacted and the network card/motherboard was replaced on 10/21/2015. [REDACTED] resumed receiving logs for the device on 10/21/2015 at 4:00 PM.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The faulty network card was replaced on 10/21/2015 and normal logging resumed in [REDACTED] for the [REDACTED] Firewall.

Provide details to prevent recurrence:

This issue occurred because of a hardware failure. This was due to the [REDACTED] device's failure to send the firewall logs to syslog and then onto [REDACTED] where they could be monitored. The issue has been resolved and mitigation steps to prevent recurrence are being investigated at this time.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

10/21/2015

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because any events that may have been logged were not able to be sent to the central logging and monitoring repository.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this possible violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 15

Record documents for the violation of CIP-005-5 R1

15.a Audit Summary

15.b The Companies' Self-Report

15.c The Companies' Self-Report

15.d The Companies' Self-Report

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-Site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

Name: [REDACTED]

Email: [REDACTED]

Standard: CIP-005-5

Requirement: R1

Sub Requirement(s): R1.3

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? ☐ Yes ☒ No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? ☐ Yes ☒ No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

Detailed explanation and cause of violation: While on-site, the audit team discovered that [REDACTED] failed to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

[REDACTED] In regards to [REDACTED] allows SNMP communication to "ANY" destination unbeknowst to the entity thus resulting in a violation of not denying all other access by default.

[REDACTED] In regards to [REDACTED] allows SNMP and FTP communication unbeknowst to the entity thus resulting in a violation of not denying all other access by default.

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Moderate

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: If the firewall rules to the ESP are configured too broadly that allows unneeded traffic inbound or outbound of the ESP, these additional routes could be use to disrupt the operations of BESCA or to allow unauthorized cyber access into the ESP itself.

Detailed description of Actual Risk to Bulk Power System: There was Minimal Impact to the Bulk Power System caused by this possible violation. This determination is due to the fact that no actual event or adverse consequences occurred.

Reference Information: [REDACTED]
[REDACTED]

Please complete the form as completely as possible and email to [REDACTED]

This item was submitted by [REDACTED] on 1/18/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.3.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered:

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation:

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

Per CIP005-5 R1, Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Electronic Security Perimeter.

R1.3 Requires inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

On 7/1/2016 the firewall team deleted two objects from the firewall policy at the [REDACTED]. Since the deleted objects were the last remaining objects in the destination field, the [REDACTED] software substituted an "ANY" designation for the destination versus a Deny All designation.

On [REDACTED] the [REDACTED] team discovered this issue when performing an ad-hoc rule review that was triggered by questions that came up during audit preparation work that was in progress at the time. They determined that the rule related to the deleted objects was not necessary and it was disabled so that the rule is not compiled into the running policy on the target device.

An extent of condition was performed by the various compliance functions within [REDACTED]. Based on review by the various groups, this issue has not transpired again within the enterprise. Either the conditions which lead to this issue have not occurred or the groups responding rely on IT to manage firewalls on their behalf. A team is currently in the process of reviewing all firewall policies and is scheduled to be complete and available for distribution in January 2017. This review includes a step to look for rules with any/any in them. At this time, only 4 firewalls have been identified as having the "ANY" designation for the destination.

The number of assets are as follows:

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal. This means that access was still limited and that protections were still being provided by other mechanisms while the erroneous rule was in place.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 1/26/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-005-5

Applicable Requirement: R1.

Applicable Sub Requirement(s): 1.3.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

[REDACTED]

Date Reported to Region or Discovered by Region:

1/18/2017

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 9/28/2017

Beginning Date of Possible Violation: 12/8/2016

End or Expected End Date of Possible Violation: 10/11/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

Per CIP-005-5 R1, each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.

Per sub-requirement R1.3, require inbound and outbound access permission, including the reason for granting access, and deny all other access by default.

On 9/28/2017, while [REDACTED] was validating decommissioned [REDACTED] it was noted that a number of BES Cyber Asset IP addresses, associated with the decommissioned systems in the [REDACTED] were not removed from the associated firewall policies, resulting in a less than adequate level of protection and non-compliance with this CIP standard, resulting in this potential violation.

Self-Assessment / [REDACTED]

On 9/28/2017, [REDACTED] was reviewing firewall policies and noted that the IP address of decommissioned systems were not removed from the respective firewall policies as part of the decommissioning process.


On 12/5/2016, the following BES Cyber Assets, identified on [REDACTED] ticketing management system for incident, change control, and alerting) [REDACTED] were marked as retired in the [REDACTED] Asset Database.

information, from applicable firewall policies, was removed by 10/11/2017.

The BES assets that were reviewed in the Extent of Condition were marked as retired in the [REDACTED] database between June 22, 2017 and December 15, 2017. Firewall policy changes have been completed and asset information removed, on [REDACTED] assets reviewed. Firewall policy changes to remove asset information on the remaining 9 BES assets are in progress.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THE PUBLIC VERSION

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Actions [REDACTED] has already completed to remediate this potential violation include:

- The required firewall policy changes have been identified and a Firewall Change Request has been submitted to implement the necessary changes. Completed 10/11/2017
- All [REDACTED] assets have been decommissioned. In addition the network environment identified in this potential violation will be decommissioned by 1/15/2018

Actions taken after performing the Extent of Condition (EOC):

Additional failures were identified while performing the EOC. These failures were attributed to [REDACTED] workflow not creating a subtask ticket to remove asset information from the associated firewall of decommissioned appliances [REDACTED]

- [REDACTED] generated a [REDACTED] report identifying decommissioned appliances that did not have a sub-ticket generated. Completed 1/12/2018
- [REDACTED] updated the [REDACTED] decommissioning workflow to generate a sub-ticket when an appliance is decommissioned. Completed 1/14/2018

Provide details to prevent recurrence:

[REDACTED] has identified the following corrective actions, and will implement these actions through the completion of the associated mitigation plan. Successful completion of the mitigation plan will prevent or minimize the probability that [REDACTED] will incur further risk of the same or similar NERC requirements in the future. Future milestones include:

- Update decommissioning process workflows for managing the decommission of [REDACTED] BES Cyber Assets
- Update the [REDACTED] document to include a [REDACTED] Asset Management Subject Matter Expert will peer check firewall policy changes associated with the [REDACTED] decommissioned assets
- Review [REDACTED] workflows to ensure appropriate sub-tickets are created, when an asset is decommissioned, to remove all asset information from all applicable firewall policies
- Update [REDACTED] workflows to ensure appropriate sub-tickets are created, when an assets is decommissioned, to remove all asset information from all applicable firewall policies
- Generate a [REDACTED] report, by asset type, to determine if a [REDACTED] sub-ticket was created when an asset was decommissioned, to ensure all asset information was removed from all applicable firewall policies
- Submit [REDACTED] sub-tickets, for any decommissioned asset, where a sub-ticket was not generated, to remove all asset information from all applicable firewall policies
- Identify individuals and perform training on updated [REDACTED] training document

See section 7.0 Corrective Actions (Fixes) Recommended by Cause Analysis Team for respective milestone dates.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

1/15/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

While [REDACTED] implementing this mitigation plan it has identified minimal risk to the reliability of the Bulk Electric System (BES).

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Risk to the Bulk Electric System:

From a BES impact standpoint this event is considered minimal because:

1) An individual with malicious intent could connect a device to the network to utilize an IP address identified in this violation which would have allowed connectivity from an unapproved asset to an asset within the Electronic Security Perimeter (ESP).

Provide detailed description of Actual Risk to Bulk Power System:

[REDACTED] did not identify any actual impact to the Bulk Electric System as a result of this potential violation and considers the likelihood of this event adversely impacting the Bulk Electric System as minimal because:

[REDACTED]

Additional Comments:

Facts, Evidence and Supporting Information:

- 1) When [REDACTED] were not migrated into the [REDACTED] tool and consequently the automated workflow incorporated into FootPrints was not utilized when [REDACTED] were being decommissioned
- 2) A process was developed ("Entering a [REDACTED] Decommission Ticket") to manage decommissioning of [REDACTED] BES Cyber Assets
- 3) A manual [REDACTED] ticket was entered on 12/8/2016 for the decommissioning of the [REDACTED] identified in the original [REDACTED] ticket
- 4) Additional [REDACTED] BES Cyber Assets were added to the original [REDACTED] ticket but not communicated to the [REDACTED] person responsible for performing the asset decommissioning process; the IP addresses remained in the policy until the discovery of this violation

Human Performance / Inappropriate Actions:

- The individual who submitted the original [REDACTED] ticket requesting assets be decommissioned added additional assets to the original [REDACTED] ticket
- The individual who added the additional assets to the original [REDACTED] decommission ticket did not communicate with the individual performing the work that additional assets were added to the ticket

Procedure Use and Adherence Investigation:

- At the time of this potential violation it was not explicitly stated in the [REDACTED] decommissioning process not to modify the original [REDACTED] ticket, once the ticket has been submitted and assigned to another person or team that changes the scope of work, without informing the assignee responsible for performing the work activity

Organizational / Programmatic Investigation:

- When [REDACTED] Assets were not migrated into the [REDACTED]

Equipment Failure Investigation:

- After performing the Extent of Condition it was determined that [REDACTED] workflow was not creating a subtask ticket to remove asset information from the associated firewall of the decommissioned appliances

An extent of condition was sent to all [REDACTED] to determine if the [REDACTED] performed firewall reviews when BES Cyber Assets were decommissioned and to identify the [REDACTED] that performs the firewall reviews on their behalf. In addition, each [REDACTED] was asked to provide a list of BES Cyber Assets (BCAs) that have been decommissioned in the past 6 months.

The [REDACTED] Lead compiled the list of decommissioned assets, identified the [REDACTED] who performed the firewall review, and selected a 10% sample of BES Cyber Assets that were decommissioned over the past 6 months.

12/14/2017: The 10% sample was sent to the respective [REDACTED] who performed the firewall review to ensure no additional failures of this nature were identified.

Conclusion: 12/20/2017: [REDACTED] identified failures while performing the test on the 10% sample. The failure to remove the asset information from the firewall was due to [REDACTED] workflow not creating a subtask ticket to remove asset information from the associated firewall of the decommissioned asset.

Per the EOC, if a failure was identified in the original 10% sample, a 25% sample of decommissioned assets is to be generated and the test re-performed.

1/9/2018: The 25% sample of decommissioned assets was generated and sent to the respective [REDACTED] to re-perform the firewall review

Conclusion: 1/12/2018: [REDACTED] identified additional failures while performing the test on the 25% sampled set of decommissioned assets.

[REDACTED] generated a [REDACTED] report identifying decommissioned appliances that did not have a sub-ticket generated to remove all asset information from the applicable firewall policies when the appliance was decommissioned. [REDACTED] is also in the process of generating the appropriate [REDACTED] sub-tickets to remove all asset information from the applicable firewall policies associated with the decommissioned appliances.

[REDACTED] updated the [REDACTED] decommission workflow to generate a sub-ticket when an appliance is decommissioned. Completed 1/14/2018

Cause Analysis:

This violation occurred as a result of the automated workflow, incorporated into [REDACTED] not being utilized when [REDACTED] BES Cyber Assets were being decommissioned.

- When [REDACTED] the decision was made not to load the [REDACTED] BES Cyber Assets into the [REDACTED] managed [REDACTED] asset management database. As a result the process that was implemented did not ensure [REDACTED] BES Cyber Assets were decommissioned properly

Cause Identification

- [REDACTED] Assets were not migrated into the [REDACTED] tool used by [REDACTED] to manage BES Cyber Assets
- The standard [REDACTED] decommissioning workflow process was not utilized
- The decommissioning process that was implemented did not ensure [REDACTED] BES Cyber Assets were decommissioned properly

The direct and contributing causes of this possible violation are as follows:

- Apparent Cause 1 (AC1): The standard [REDACTED] decommissioning workflow process was not utilized because [REDACTED] assets, identified in this potential

violation, are not in the [REDACTED] asset database

• Contributing Cause 1 (CC1): Additional assets were added to a [REDACTED] change ticket after the original ticket was submitted to be worked

• Contributing Cause 2 (CC2): [REDACTED] did not have a policy stating that changes to any [REDACTED] ticket, which has been submitted and assigned to another person or team, shall not be modified in a way that changes the scope of work without informing the assignee(s) responsible for performing that work activity

• Contributing Cause 3 (CC3): [REDACTED] workflow did not create sub-tickets for decommissioned appliances

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/7/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.5.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/28/2017

Beginning Date of Possible Violation: 1/11/2017

End or Expected End Date of Possible Violation: 3/1/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

On 2/15/2017, a review of the [REDACTED] which is a [REDACTED] was conducted to ensure all compliance controls remained in effect and operational following a scheduled and approved change that was completed on 1/11/2017.

[REDACTED] completed on 1/11/2017 was a scheduled and approved change to decommission End of Life [REDACTED] located in the [REDACTED] by replacing with new [REDACTED]. During the change, data cables connected between IDS TAPs and the [REDACTED] being decommissioned were inadvertently overlooked and not moved to the new [REDACTED]. As a result, a possible violation of CIP-005-5 R1.5 was identified.

On 3/2/2017 the last of three scheduled and approved changes were implemented to install all IDS TAPs and confirm traffic inbound and outbound for the defined ESP is being forwarded to and monitored by IDS, ending the possible CIP violation timeframe that began 1/11/2017.

Are Mitigating Activities in progress or completed? Yes

An Informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

Mitigation activities that have been completed:

1. Completed scheduled and approved changes on 2/28/2017, 3/1/2017, and 3/2/2017, to install all IDS TAPs and confirm traffic inbound and outbound for the defined ESP located at the [REDACTED]s being forwarded to and monitored by IDS.

Mitigation activities scheduled to be completed:

1. Complete a review of all High Impact BES Cyber Systems and Medium Impact BES Cyber Systems located at Control Centers to confirm compliance with the CIP-005-5 R1.5 requirement.

2. Implement a labeling methodology to clearly identify data network connections that include Test Access Points (TAPs). Expected completion Date: 4/10/2017

3. Determine 1) Who within [REDACTED] has the responsibility to monitor IDS and 2) Respond to security events reported by IDS to ensure they are being addressed. (This event identified a gap in responsibility that when addressed, will more quickly identify if / when a TAP has been inadvertently removed)

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

Complete an Apparent Cause Analysis to further identify mitigation activities to prevent recurrence. The ACA may identify recommendations to more clearly identify the location of TAPs, improve the Change Control Process, or implement additional Human Performance tools to avoid an oversight when implementing a change.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/28/2017

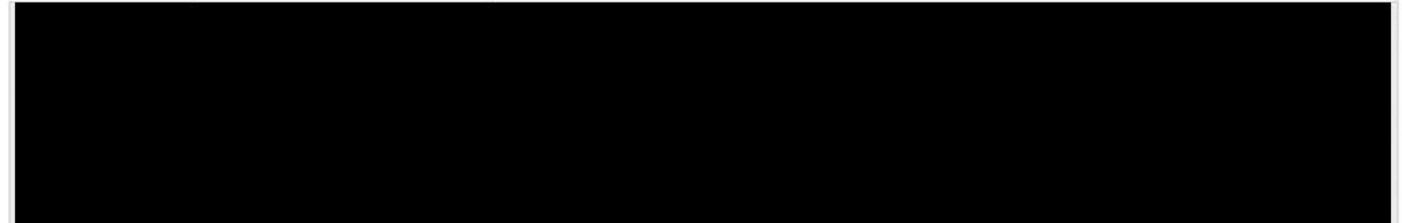
MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:



Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System associated with this possible violation. No mis-operations, emergencies, or other adverse consequences to the Bulk Power System resulted from this event.

In addition, no alerts were captured or invalid login attempts were recorded by [REDACTED] Tools for any Cyber Assets associated with the possible violation and no malicious communication was flagged by IDS.

Additional Comments:

[Redacted area for Additional Comments]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 16

Record documents for the violation of CIP-005-3a R2.1, R2.2, R2.4

16.a The Companies' Self-Report

16.b The Companies' Self-Report

16.c The Companies' Self-Report

This item was submitted by [REDACTED] on 7/25/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.3.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

1/23/2017

Monitoring Method for previously reported or discovered:

Self-Certification

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/20/2017

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 6/20/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Registered Entity(s) SR Applies to: [REDACTED]

On 6/20/17, during the Network Discovery element of an Active Cyber Vulnerability Assessment (CVA) at the [REDACTED] of [REDACTED] location, a potential violation was self-identified where [REDACTED]

Upon investigation, it was determined that [REDACTED]

To ensure no other CIP controlled locations were impacted, an Extent of Condition was completed that involved a physical walk down of all [REDACTED]. It was confirmed that two locations could have possibly led to a compromise. A change request - [REDACTED] - was initiated and completed on 6/22/2017 to correct the misconfiguration identified at the [REDACTED]. On 6/26/2017, a change request - [REDACTED] was initiated to correct the misconfiguration identified at the [REDACTED] and completed on 6/27/2017.

When the change that prompted this possible violation was implemented in May 2012, no formal change control process existed for CIP devices. Therefore, no checks

and balances were in place to ensure a change was properly reviewed and vetted to prevent a potential negative impact to [REDACTED]

To prevent recurrence of the possible violation, [REDACTED] will continue to use and enhance change control processes implemented July 1, 2016 as part of NERC CIP Version 5 deployment. Additionally, for [REDACTED] devices located within an Electronic Security Perimeter, this process requires [REDACTED] which implements separation of duties practices. The BES Change Control Form is an archival document where evidence is attached and confirmed to have no impact or comprise on security controls during change implementation. [REDACTED]

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

A cause analysis will take place to identify additional actions to prevent recurrence of this possible violation.

[REDACTED]

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is moderate, due to the fact that if the unprotected virtual hosts had been configured to allow communication to ESP networks, mal-ware, virus, or someone with malicious intent would have had access to systems located within the ESP, which could have potentially impacted the availability and/or operation of the Bulk Electric.

[REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the possible violation.

Additional Comments:

[REDACTED]

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 6/22/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-005-3a

Applicable Requirement: R2.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/13/2017

Beginning Date of Possible Violation: 1/18/2016

End or Expected End Date of Possible Violation: 5/30/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

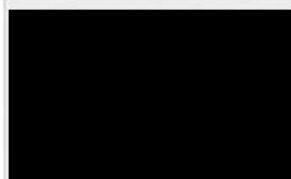
This Self-Report applies to [REDACTED]
Per CIP5-3a R2.2: At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

On 4/13/2017 during preparation for performing work to remove existing [REDACTED] printer queues from the [REDACTED] related print servers [REDACTED] located at the [REDACTED] it was discovered that [REDACTED] was no longer connected to the corporate network. Subsequent conversations with the Sr. Print Services Consultant surfaced that the printer was replaced with a new Xerox printer on 1/18/2016 and the decision was made to no longer provide EMS printing at that particular physical printer location.

However, the firewall rules were never updated to remove the egress for [REDACTED]. Therefore, this was an unauthorized egress point. It began on 1/18/2016 and the unauthorized egress point had not been removed. A Firewall Filter Change Request (FFCR) to have the firewall updated following the removal of this printer was not made until 4/17/17.

[REDACTED] was completed on 4/28/17 removing [REDACTED] printing support from [REDACTED] therefore, removing the egress point.

A cause analysis will take place to assist in preventing recurrence of this possible violation.



Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal due to the following:

- The open firewall rule permits egress to an IP network that is only present within [REDACTED] Physical Secure Perimeter located at the [REDACTED]

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Mitigating factors include:

- A [REDACTED] workstation is required in order to access the [REDACTED] on which the printer resided
- [REDACTED] workstations are scanned for malicious software
- [REDACTED] laptops are encrypted
- IDPS devices are deployed, alerting to malicious communication into the ESP
- The firewall rules were removed once the gap was discovered

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 8/28/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-3a

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.5.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

2/23/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 5/20/2015

Beginning Date of Possible Violation: 5/20/2015

End or Expected End Date of Possible Violation: 5/20/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

While working on a previous mitigation plan [REDACTED] for a violation in regards to the Q1 quarterly access review, the Q2 quarterly access review was also underway. The Q2 quarterly access review was compared to the user access list and account information was found to have not been updated in 7 calendar days as required by CIP-004 R4. Those discrepancies were found and corrected right away as follows:

The following were corrected to document account removal:

[REDACTED] - Account was removed but no notification of removal was received so removal wasn't documented to list.

[REDACTED] Access to [REDACTED]

The following were removed from the Server Admins group from:

The following was added to the [REDACTED] Audit Reports group:

[REDACTED] - Notification was not provided in order to update list.

Documented [REDACTED] access for: (this allows for 2ndary authentication to occur, but by itself doesn't provide any access)

[REDACTED] - Access to [REDACTED] server did not exist prior quarter. I believe this to be an issue with the account. The issue was corrected but I was not notified of the resolution

and thus creation of the [REDACTED] account.

Documented the addition of the accounts- Found creation ticket [REDACTED] (created to reset passwords and prepare for support changes). This work management system does not provide me notifies regarding account changes. I was not notified of the account creation at the time.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Documented account [REDACTED] for when it was added and when it was removed. The account was created by a [REDACTED] member unfamiliar of all of the compliance activities around new account creation [REDACTED]

03/15/2015 - Added new shared account - 04/24/2015 - [REDACTED] - Removed account

The cause of this violation is due to manual maintenance of an isolated list which has been prone to error and provided no benefit over reviewing approved access via the system of record and approval documentation which we will be migrating to. Also, this mitigation plan will help ensure that future terminations lead to direct notification regarding the need to remove EACM access. This will ensure better compliance and stronger protection of the BPS.

Are Mitigating Activities in progress or completed? ☒ Yes

If Yes, Provide description of Mitigating Activities:

A review of the second quarter access reporting and the user access list was completed on June 9th, 2015. On that same day, the HR system was updated to add a CIP flag to HR records for all individuals with EACM access. That change ensures that reporting of daily terminations will provide alerting regarding individuals with EACM CIP access. That reporting will alert access services of the need to review and remove the individuals' CIP access.

On 8/31/2015, the user access list process will be migrated to reference the system of record. This removes the extra administrative step of maintaining a separate list which provides no extra value. This also helps align user access review processes to ensure consistency and avoid parallel processes that cause confusion.

On 8/31/2015, a notification will be sent out to the parties affected by the above change to ensure they are aware of the change and the switch to a more unified process based on one they are already familiar with and performing for the majority of the accesses they manage (e.g., this new process was already in place for [REDACTED]).

Provide details to prevent recurrence:

Successful completion of this Mitigation Plan will prevent or minimize the probability that [REDACTED] incurs further risk of alleged violations of the same or similar reliability standards requirements in the future. The actions performed in this mitigation plan will remove the manual maintenance of an isolated list which has been prone to error and provided no benefit over reviewing approved access via the system of record and approval documentation which we will be migrating to. Also, the mitigation plan will help ensure that future terminations lead to direct notification regarding the need to remove EACM access. This will ensure better compliance and stronger protection of the BPS.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/31/2015

Potential Impact to the Bulk Power System:

Actual Impact to the Bulk Power System:

Provide detailed description of Potential Risk to Bulk Power System:

While [REDACTED] is implementing this Mitigation Plan, it has identified no risks or impacts to the reliability of the BPS because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation

Provide detailed description of Actual Risk to Bulk Power System:

No misoperations, system operating limits, or interconnection reliability operating limits occurred as a result of this violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Attachment 17

Record documents for the violation of CIP-005-5 R2

17.a The Companies' Self-Report [REDACTED]

17.b The Companies' Self-Report [REDACTED]

17.c The Companies' Self-Report [REDACTED]

17.d The Companies' Self-Report [REDACTED]

17.e Audit Summary [REDACTED]

17.f The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

2.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 12/30/2016

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

This Applies to [REDACTED] upon conducting audit preparation review activities of the 'Access Rule Review' documentation describing the allowed communication paths contained in the Firewalls and Core Routers at [REDACTED] it was discovered that Interactive Remote Access was allowed from each of the generation units [REDACTED] to the [REDACTED] a medium impact BES Cyber System. Access to a medium impact BES Cyber System requires the use of an Intermediate System. The communication path at [REDACTED] does not have the required Intermediate System.

Due to the existing mitigating measures, in place upon commission date of [REDACTED] at the [REDACTED] the risk to the BES Cyber System is minimized. The mitigating measures existing at the time of the incident are listed below.

[REDACTED]

Extent of Condition activities have been performed.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because of the mitigating measures currently existing at the time of the incident. Personnel having the ability to remotely access devices have the proper training, personnel risk assessment and are knowledgeable of NERC CIP procedures.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered:	No
---	----

No

Has this Possible Violation previously been reported to other Regions: No

No

Date Possible Violation was discovered:

Beginning Date of Possible Violation: 7/1/2016

7/1/2016

End or Expected End Date of Possible Violation:	12/31/2016
---	------------

12/31/2016

Is the violation still occurring? Yes

Yes

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]
Per CIP-005 R2:

Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one of more documented process that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 - Interactive Remote Access Management.

██████████ performed an initial identification of Intermediate Systems supporting Remote Interactive Access through the CIP V5 implementation program in May 2015. The infrastructure was identified as the Intermediate System and key components of that infrastructure were classified as EACMS at that time.

During audit preparation review sessions in [REDACTED] with newly formed QA teams, [REDACTED] reassessed the specific systems within the [REDACTED] environment that perform required components of the Intermediate System functionality and determined that it was appropriate to include the [REDACTED] servers that provide the [REDACTED]

Two potential violations were identified related to the inclusion of these additional devices in the Intermediate System.


Issue #1:

Intermediate Systems providing Remote Interactive Access to devices within Electronic Security Perimeters (ESP) at the [REDACTED] resided within those ESPs, contrary to the defined attribute of Intermediate Systems that they must reside outside the ESP boundary. [REDACTED] servers were identified.

Issue #2:

Certain servers serving as Intermediate Systems providing Remote Interactive Access to devices within Electronic Security Perimeters at multiple [REDACTED] and [REDACTED] were not initially identified as EACMS, contrary to the defined attribute of EACMS that they include Intermediate Systems. [REDACTED] servers were identified.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The mitigating activities [REDACTED] has taken are as follows:

Initial meetings were held on 8/3 and 8/4 to discuss the current state of the system.

Additional research was conducted on 8/8 that confirmed the presence of the PV. Planning for required architecture changes has been initiated and changes to the new ESPs being built going forward.

Asset Inventory updates for the [REDACTED] misclassified assets has been initiated and documentation updates are underway.

Initial discussions of what protections are currently in place for newly identified EACMS have taken place and initial plans to deploy the full compliance program have been discussed.

Provide details to prevent recurrence:

Additional actions will be determined during development of the mitigation plan.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

3/31/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Initial Meetings	8/3/2016	Discuss the Current State of System.	No
Initial Plan Development	9/6/2016	Project Plan Timeline	No
Architecture Review	12/5/2016	Network Topology	No
Implementation	3/3/2017	Mitigating Steps	No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because the assets are currently receiving the required physical and electronic protections of an EACMS.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.3.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered:

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 9/30/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self Report applies to [REDACTED]

Per CIP005-5 R1, Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Electronic Security Perimeter.

R1.3 Requires inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

During audit preparation reviews of EAP rule sets on [REDACTED] it was discovered that there was the potential for user access into [REDACTED] ESP (Electronic Security Perimeter) networks.

[REDACTED]

Four (4) firewalls were identified as in scope at this time; two (2) are located at the [REDACTED] and two (2) are located at [REDACTED]. To determine extent of condition, a firewall rule policy review is underway for all NERC CIP firewalls and is scheduled to be complete and available for distribution in January 2017.

For the [REDACTED] policy:

[REDACTED]

For [REDACTED] Firewall policy:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

The number of assets is as follows:

The number of assets is as follows:

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal. There is no direct access to the firewall without user credentials which requires two factor authentication and a user profile in [REDACTED] for access to the specific firewalls. The access to the firewall rules are limited due to the "deny all" rule at the end of each rule.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED]

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-005-5

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: 9/9/2016

Monitoring Method for previously reported or discovered: Self-Report

Has the scope of the Possible Violation expanded: Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 3/29/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

This situation was originally identified during the [REDACTED] At that time [REDACTED] was performing an initial identification of Intermediate Systems supporting Remote Interactive Access and determined that it was appropriate to include additional elements of the [REDACTED] environment in the definition of Intermediate System. As a result a potential violation 43896 and [REDACTED] was submitted.

At that time [REDACTED] did not have a defined procedure for reviewing all remote access mechanisms and the associated EAP access rules or policy statements. The review was focused specifically on the use of Interactive TCP/IP ports/protocols as well as the specific sources used to access assets within any defined ESP. To mitigate this issue, [REDACTED] updated their procedure to include new steps to review for Interactive Remote Access conditions and to ensure all connections utilize Intermediate Systems for access to an ESP.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

While [REDACTED] was performing the ongoing annual firewall review it was determined that access was provisioned and approved, as required prior to July 1, 2016, providing direct access to cyber assets without utilizing an Intermediate System. Changes were not made to preclude the direct interactive remote access connectivity prior to the Electronic Security Perimeter commissioning as part of the EMS Upgrade project in the [REDACTED] in accordance with the noted NERC CIP v5 requirement.

This issue was discovered during the annual firewall policy reviews, which included the new interactive remote access reviews, of the [REDACTED] Critical Infrastructure firewall policies.

On March 29, 2017 steps were implemented to resolve this potential violation by submitting the appropriate firewall filter change requests (FFCR) and [REDACTED] Change Request (CRQ).

A cause analysis will be schedule to assist in preventing recurrence of this potential violation.

Associated Asset / BES Cyber System Count of Classification Tier



Provide detailed description of Actual Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because direct access to the ESP is limited to specific support engineers and Infrastructure/Application subject matter experts who have been trained and screened for NERC CIP electronic access.



Additional Comments:

There was no Actual Impact to the Bulk Power System caused by this possible violation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Post On-site Audit/Off-site Audit/Spot Check/Investigation Screening Worksheet

Prepared By: [REDACTED]

Submittal Date: [REDACTED]

Compliance Monitoring Method (On-site Audit, Off-site Audit, Spot-Check, or Investigation):
On-Site Audit

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

Registered Entity Contact Information:

[REDACTED]

Standard: CIP-005-5

Requirement: R2

Sub Requirement(s): R2.1

Function(s) Applicable to Possible Violation:

[REDACTED]

Date violation occurred: 07/01/2016

Date violation discovered (Exit Presentation Date): [REDACTED]

Is the violation still occurring? ☐ Yes ☒ No

Are mitigating activities (including details to prevent reoccurrence) in progress or completed? ☐ Yes ☒ No

If yes, Provide description of Mitigating Activities:

Date Mitigating Activities are expected to be completed or were completed:

Detailed explanation and cause of violation: While on-site, the audit team discovered that [REDACTED] failed to utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

Potential Impact to the Bulk Power System (Minimal, Moderate, or Severe): Moderate

Actual Impact to the Bulk Power System (Minimal, Moderate, or Severe): Minimal

Detailed description of Potential Risk to Bulk Power System: If the ACLs to the ESP are configured too broadly that allows unneeded traffic inbound or outbound of the ESP, these additional routes could be used to disrupt the operations of BESCAs or to allow unauthorized cyber access into the ESP itself.

Detailed description of Actual Risk to Bulk Power System: There was Minimal Impact to the Bulk Power System caused by this possible violation. This determination is due to the fact that no actual event or adverse consequences occurred.

Additional Comments: Reference Information: [REDACTED]

Please complete the form as completely as possible and email to [REDACTED]

This item was submitted by [REDACTED] on 8/8/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-005-5

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

2.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

6/22/2017

Monitoring Method for previously reported or discovered:

Self-Certification

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 6/26/2017

Beginning Date of Possible Violation: 6/23/2017

End or Expected End Date of Possible Violation: 6/30/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

CIP 005 5 R2.1: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

[REDACTED]

The ticket request [REDACTED] was completed and disabled the firewall rule on 6/26/2017.

Source Systems: Intermediate Remote Access was possible from the following new Cyber Assets which have not been commissioned:

A cause analysis will be performed to identify additional actions required to prevent recurrence of this type of potential violation.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the possible violation.

Additional Comments:

Attachment 18

Record documents for the violation of CIP-006-3c R1

18.a The Companies' Self-Report [REDACTED]

18.b The Companies' Self-Report [REDACTED]

18.c The Companies' Self-Report [REDACTED]

18.d The Companies' Self-Report [REDACTED]

18.e The Companies' Self-Report [REDACTED]

18.f The Companies' Self-Report [REDACTED]

18.g Audit Summary [REDACTED]

18.h The Companies' Self-Report [REDACTED]

18.i The Companies' Self-Report [REDACTED]

18.j The Companies' Self-Report [REDACTED]

18.k The Companies' Self-Report [REDACTED]

18.l The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 6/13/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-006-3c

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

3/12/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 3/18/2016

Beginning Date of Possible Violation: 3/4/2016

End or Expected End Date of Possible Violation: 3/23/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

[REDACTED] was performing construction and renovation work at the [REDACTED] involving the installation of HVAC supply and return vents through an existing NERC CIP PSP boundary/wall. When the work was initially completed, the vents were not properly secured to prevent unauthorized physical access into the PSP. The breach occurred on March 4, 2016, was discovered on Friday, March 18 and was temporarily mitigated the same day by [REDACTED] over each of the openings. [REDACTED]

This event is a potential violation because the PSP was not secure. Per CIP-006-3c R1.1, "All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter." Since the vents were not properly secured to prevent unauthorized physical access into the PSP, this was considered a breach.

***At the time of this possible violation, the site in the [REDACTED] region, had the following Critical BES Cyber Asset devices present:

Site in scope: [REDACTED]

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The breach was discovered on Friday, March 18 and immediate corrective action was taken the same day by [REDACTED] over each of the AC duct openings. [REDACTED]

Provide details to prevent recurrence:

Future recurrence will be prevented by reinforced training and enhancements to change control processes.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

3/23/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because immediate corrective action was taken on March 18, the same day of discovery. The corrective action was [REDACTED] over each of the AC duct openings. [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power system caused by this alleged violation because there were no misoperations, emergencies or other adverse consequences to the Bulk Power system as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 7/21/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.5.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

1/4/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/16/2015

Beginning Date of Possible Violation: 4/16/2015

End or Expected End Date of Possible Violation: 4/16/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-004-3a R4, [REDACTED] shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. [REDACTED] uses the [REDACTED] systems when processing access requests in order to help ensure compliance with this standard. An issue was noted on 4/16/15 related to the processing of the access request and the following are the details of it.

1. A [REDACTED] ticket was submitted for one individual requesting access to one Physical Security Perimeter (i.e., the [REDACTED] Non-PSP Server Room.
2. Upon validation of PRA and training [REDACTED] submitted an electronic request form to the Badge Office on 04/13/2015. The Badge Office is responsible for authorizing the physical access to the various [REDACTED] locations.
3. The Badge Office processed the electronic form on 4/16/15.
4. Access was inadvertently granted to the Physical Security Perimeter [REDACTED] at 3:07 PM on 4/16/15 instead of the [REDACTED] Non-PSP Server Room as requested. The error was noted as part of [REDACTED] process of confirming completed badge access requests.
5. An e-mail was sent to Badge Office notifying them of the mistake (i.e., the inadvertent access to the [REDACTED]).
6. [REDACTED] access was removed for the one individual at 3:26 p.m. on 4/16/15.

At the time of the possible violation, there were [REDACTED] critical cyber assets potentially exposed in the area for which the employee did not have access to.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Yes, the mitigating actions are complete. The Incorrect physical access was removed upon detection. It should be noted the access was only in place for a period of 19 minutes.

Provide details to prevent recurrence:

[REDACTED] has implemented a new [REDACTED] that replaced the prior online systems [REDACTED] for requesting enterprise badges and facility access. The new system automates much of the manual functions used in the former processes to help prevent reoccurrence of similar issues in the future.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/16/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal. This was not an operational issue that could affect reliability of the Bulk Power System. Please refer to mitigating activities section above for further details of actions taken to resolve this issue.

Provide detailed description of Actual Risk to Bulk Power System:

This alleged violation was not the result of an intentional action to violate a NERC reliability standard. Rather, [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard. It is evident that [REDACTED] was attempting to comply as evidenced by correcting the inadvertent access granted approximately 19 minutes after it occurred.

Additional Comments:

This alleged violation was not the result of an intentional action to violate a NERC reliability standard. Rather, [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard. It is evident that [REDACTED] was attempting to comply as evidenced by correcting the inadvertent access granted approximately 19 minutes after it occurred.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 10/28/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R4.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

12/29/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 7/24/2015

Beginning Date of Possible Violation: 7/21/2015

End or Expected End Date of Possible Violation: 8/21/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Per CIP-007-3a R5.1.1 [REDACTED] is obligated to ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

[REDACTED] standard NERC access request procedure is as follows:

1. Individual's supervisor/manager submits a request into [REDACTED] badge access tool (this is considered the first level of approval)
2. [REDACTED] the group that verifies training and PRRS receives a notification that a request has been submitted
3. [REDACTED] emails the appropriate Space Access Approver for the requested site with details included in the access request.
4. Space Access Approver replies with approval or rejection
5. [REDACTED] takes action in [REDACTED] access management tool accordingly.

Issue #1

On 7/17/15 a [REDACTED] contractor requested access to two NERC locations, in the [REDACTED], using the [REDACTED] physical access request tool: [REDACTED]

Each PSP has a designated [REDACTED] who reviews request for access and communicates his decision to [REDACTED]. [REDACTED] is responsible for maintaining [REDACTED] access lists and formally approving physical and electronic access upon request. The [REDACTED] approved access to the [REDACTED] and denied access to the [REDACTED] Area.

On 7/21/15, [REDACTED] personnel approved the request in (in error). The intent was to reject the request. The [REDACTED] individual selected "approve" rather than "deny."

On 7/24/15, the error was discovered as a result of checking the daily [REDACTED] report. The report is designed to identify any [REDACTED] or [REDACTED] of [REDACTED] situations or regards to NERC access. [REDACTED] noticed this particular individual was granted access to both locations while access should have been denied at [REDACTED] Area. This error was corrected immediately by removing the incorrect access following the discovery.

UNCLASSIFIED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

A report from [REDACTED] badging office for the individual shows the contractor did not access [REDACTED] Area during the timeframe of 7/21/15-7/24/15.

Issue #2

On 8/21/2015 a contractor entered a [REDACTED] request for access to [REDACTED] NERC locations at the [REDACTED] Access was requested for a [REDACTED] administrator who was going to be working temporarily at the [REDACTED] NERC locations.

[REDACTED] did not send the access request to the SAAs for approval before inadvertently approving the request on 8/21/2015. The error was noticed and corrected immediately.

A report from [REDACTED] badging office for the individual shows the contractor did not access [REDACTED] on 8/21.

Are Mitigating Activities in progress or completed? ☒ Yes

If Yes, Provide description of Mitigating Activities:

Issue #1

The [REDACTED] EMS Area was removed on 7/24/15 at 3:40 p.m.

Issue #2

[REDACTED] were removed on 8/21/2015. The access was removed immediately upon determination of the error. Access was granted on the badge for less than one hour.

Provide details to prevent recurrence:

[REDACTED] is conducting research into [REDACTED] process of provisioning access to determine the cause behind the errors.

Immediate corrective action was complete 7/24 and 8/21 respectively.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/21/2015

Potential Impact to the Bulk Power System:

Actual Impact to the Bulk Power System:

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because:

Issue #1

The individual's training and Personnel Risk Assessment (PRA) are up to date. Also, the error was identified and corrected three (3) days later.

Issue #2

The individual's training and Personnel Risk Assessment (PRA) are up to date. The error was identified and corrected within an hour

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Issue #1

A report from the badging office for the individual shows the contractor did not access [REDACTED] Area during the timeframe of 7/21/15-7/24/15.

Issue #2

A report from the badging office for the individual shows the contractor did not access [REDACTED] on 8/21.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 3/11/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-004-3a

Applicable Requirement: R4.

Applicable Sub Requirement(s): [REDACTED]

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 10/13/2015

Beginning Date of Possible Violation: 9/28/2015

End or Expected End Date of Possible Violation: 11/5/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This Self-Report applies to [REDACTED]

Per CIP-004-3a-R4, [REDACTED] is obligated to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs.

On 09/28/2015 at 11:24am, a [REDACTED] manager submitted an access request for a subordinate via the [REDACTED]. The request had four non-Physical Security Perimeter (PSP) access levels to remove and one NERC PSP access to add. As of the date of the request, an add and remove request in the same ticket was not allowed.

At 11:25am the non-PSP access was automatically removed by the tool. At 13:42pm, an [REDACTED] Analyst discovered that the [REDACTED] had provisioned badge access to an employee's badge for a NERC PSP after it had been manually rejected. The request for access was manually rejected by an [REDACTED] Analyst because [REDACTED] does not allow removals of site access and additions of NERC PSP access in the same request.

At 23:07pm, a contractor in the [REDACTED] logged into [REDACTED] as a System Administrator and re-rejected this request due to system issues. At this point, the [REDACTED] believed that the [REDACTED] employee's access was rejected. It was later discovered that [REDACTED] provisioned access prior to the confirmation email from the Site Authorized Administrator, giving permission for the employees access to be added to the NERC PSP.

The following day (09/29/2015), the system automatically generated an anomaly report and sent it to an [REDACTED] Analyst but it was not read until 10/13/2015. The anomaly report presented findings of potential issues which included the [REDACTED] employee's rejected request. Upon reading the report, the [REDACTED] Analyst notified the [REDACTED] that the rejected access showed up in [REDACTED]. This was verified by the [REDACTED] who also discovered it in [REDACTED]. The company is currently switching to [REDACTED]. A contractor in the [REDACTED] then removed the NERC PSP access from the account from [REDACTED]. The [REDACTED] also confirmed that access never showed up in employee's [REDACTED] profile.

The [REDACTED] had the proper Personal Risk Assessment (PRA) and Cyber Security training to request NERC PSP access but the system tool [REDACTED] provisioned access prior to the confirmation email from the Site Authorized Administrator. This allowed employee access to that particular PSP. The cause for this incident was a coding error within the [REDACTED] application.

At the time of this potential violation only one NERC access category was granted wrongfully which included two High NERC PSP's. One was entered and one was not.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

After the coding error in [REDACTED] was identified, IT made changes to the tool, separating [REDACTED] from the Physical Access Controls (PACS) to ensure that an add/remove request in the same ticket did not incorrectly grant access to NERC PSP's.

Provide details to prevent recurrence:

The coding within [REDACTED] has been changed and tested, negating the possibility of the same internal tool error in the future.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/5/2015

Potential Impact to the Bulk Power System: Severe

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is serious because at the time of this potential violation, [REDACTED] managed access to all [REDACTED] authorized NERC PSP access points with card readers; therefore, all [REDACTED] NERC PSP's were at vulnerable to unauthorized access after a request for access had been requested. Six individuals have been identified as receiving NERC PSP access through this coding error, although all had proper PRA and Cyber Security Training. Site Authorizations were also granted, however, it was after [REDACTED] had provisioned the access.

Provide detailed description of Actual Risk to Bulk Power System:

The Actual Impact to the Bulk Power System is minimal because the subjects who gained access to the NERC PSP's via the [REDACTED] coding error all had proper PRA and Cyber Security Training. All individuals were accessing the site in accordance with their job duties and had site approval. The site approval was delayed due to the method of communication (e-mail), therefore; resulting in a potential violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Manual Log in place at the control center, as well as training, and reviews of Manual Logs.

No [REDACTED] internal compliance plan that was in effect at the time of the potential noncompliance could have prevented the potential noncompliance.

There were no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 5/19/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-006-3c

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: 1/6/2014

Monitoring Method for previously reported or discovered: Self-Report

Has the scope of the Possible Violation expanded: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 3/17/2015

Beginning Date of Possible Violation: 3/14/2015

End or Expected End Date of Possible Violation: 4/30/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

In accordance with CIP-006 R1.6 and specifically 1.6.1, [REDACTED] is required to have a visitor control program for visitors containing at a minimum: 1) Logs to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

On 3/17/15, a review of [REDACTED] Physical Security Perimeter (PSP) visitor logs was performed. It was discovered that on 3/14/15 and 3/17/15, no manual log entries were completed for two visitors.

INCIDENT #1: An employee with authorized unescorted access came into [REDACTED] (inside the [REDACTED] PSP) on 3/14/15 with her husband and daughter but did not complete manual log entries for that time period.

INCIDENT #2: On 3/17/15 at approximately 11:00AM, the same employee brought her husband into the Operations Manager's office in the [REDACTED]. After they left, it occurred to the Ops Manager that the husband did not have a Visitor badge. He then checked the logs and found an incomplete entry. Upon further review, it was determined that the employee had also failed to log entries during the 3/14/15 visit to the [REDACTED].

[REDACTED] has established procedures for visitor control, CIP006 R1.6 Visitor Control Program (which is posted as "Good Security Practices" on [REDACTED] internal website) and CIP-006 R1.6 Procedure for Escorted Access Within the Physical Security Perimeter. The procedures require visitors to be provided Visitor Badges and visitor information be recorded in the the visitor log upon entry and when exiting the PSP.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken with respect to this issue include the following:

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

1. To focus on the importance of logging, [REDACTED] developed Q12015 Security Awareness reinforcement around visitor management and updated the Visitor Management poster. This quarterly reinforcement was issued 03/22/15 along with copy of the poster to all persons with CIP access.
2. A follow-up communication was sent 4/01/15 from [REDACTED] to ensure all of [REDACTED] is aware of the visitor management program.
3. On 4/30, [REDACTED] Operations Manager informed [REDACTED] staff of instances noted in logging that did not fully meet the requirements and requested their review of the Manual Log Completion Basics training presentation as a reminder.

Provide details to prevent recurrence:

A follow-up communication was sent 04/01/15 from [REDACTED] to ensure all of [REDACTED] is aware of the visitor management program.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/30/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact is minimal because in both instances the visitors were continuously escorted during the time of the issues. The potential risk is that without complete log entries and visitor badges, [REDACTED] may be unable to uniquely identify a visitor or know the exact times the visitor entered or exited the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

The actual impact to the Bulk Power System (BPS) caused by this possible violation is minimal because in both instances the visitors were escorted the entire time and did not access the console.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 7/21/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-006-3c

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

8/5/2014

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/7/2015

Beginning Date of Possible Violation: 4/7/2015

End or Expected End Date of Possible Violation: 4/7/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This possible violation is for [REDACTED]

In accordance with the [REDACTED] is required to have a visitor control program containing logs [REDACTED]. These manual logs are to be used for persons without authorized access to the PSP. This is further defined in the CIP006 R1.6 Procedure for Escorted Access within the Physical Security Perimeter (V4, dated 6/24/13) which requires visitor logs to be used to document the entry and exit of visitors, including the date and time, to and from the PSPs.

The procedure further spells out in Section 4, Page 2 to "Ensure that designated escorts sign in their visitors using the Visitor Log book provided at each Physical Security Perimeter at the beginning of their work day and at the conclusion of their work scope or work day whichever comes first."

Site visits were setup to take a group of people to two [REDACTED] in the [REDACTED]. A list of people had been established and access requests had been submitted for the team of people. A contractor was added to the team for [REDACTED] site visits but was not included in the access requests for the initial team.

On April 7, 2015, while at [REDACTED], two issues occurred.

Issue #1

On 4 April 7, 2015/7/15, the contractor, along with the rest of the team, went to the sites with the understanding that anyone without authorized access would be escorted by

the [REDACTED] escort or another member of the team who was authorized to serve as the NERC CIP escort.

When the team arrived in [REDACTED] Tuesday morning, their [REDACTED] contact tested the badges of the group to see whether they had access to the [REDACTED] floor. The badge reader showed Green when contractor's badge was swiped. This was after swiping several other [REDACTED] badges which also showed Green on the badge reader.

REDACTED INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

It was assumed that the contractor had unescorted physical access.

At one point contractor stepped out of the PSP to use the restroom. When he tried to reenter the PS his badge did not work. It was at this point in time he realized he did not have authorized unescorted access to the PSP.

Due to this incident, [REDACTED] is in possible violation to CIP-006 R1.6.1 and CIP-006 R1.6.2.

At the time of this incident the contractor had a current PRA but had not completed the PSP training.

Issue #2

While reviewing the April 7, 2015 electronic log it was determined, in addition to the contractor who did not have unauthorized access privileges, a [REDACTED] employee also lacked the appropriate authorization to have unescorted physical access to the same PSP [REDACTED]. The [REDACTED] employee had physical access to the [REDACTED] site just not the [REDACTED] site. The [REDACTED] employee stayed with the escort through the site visit in [REDACTED].

Review of the physical log for that date/location indicated that neither individual created an entry in the manual visitor log.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Issue #1

Wednesday morning, April 8, 2015, the leadership team in [REDACTED] was alerted to the fact that the contractor's badge was swiped and contacted the team in Indiana.

The contractor was instructed to stop swiping his badge immediately and to sign in per the visitor processes.

The contractor confirmed that he signed in appropriately for Wednesday at the [REDACTED] location; however he did not sign the manual visitor log in [REDACTED] location on Tuesday.

The team confirmed that the contractor was escorted when within a [REDACTED] PSP at all times by someone with authorized unescorted physical access.

A note was sent to the team reiterating appropriate use of badges in the [REDACTED] to clarify that they should not rely on "testing" their badges to determine whether they work.

Upon investigation the contract vendor removed the contractor from the [REDACTED] account.

Issue #2

On April 21, 2015 the appropriate NERC access form was submitted for the [REDACTED] employee requesting unescorted physical access to the [REDACTED] site.

Provide details to prevent recurrence:

[REDACTED] is currently implementing an enterprise project called CIP Transformation that includes an enhanced visitor control program to maintain and strengthen support and compliance to NERC CIP-006. This enhanced visitor control program includes updated procedures and clarifies requirements on visitor logging and visitor log maintenance. These procedures were designed to incorporate improved controls to detect potential issues and prevent them from occurring.

As part of the CIP Transformation, a revised Computer Based Training (CBT) program trains individuals on the appropriate use and responsibilities of having unescorted physical access to a PSP. Training also includes responsibilities for someone who has physical unescorted access when an individual without that access must enter the PSP.

In addition a training CBT has also been implemented instructing individuals on the appropriate procedure for completing the Manual Visitor Log.

Updated the current training material to include a slide instructing users who enter a PSP, via a card reader that controls access to the PSP, to make sure the door is closed and the card reader is "reset" before the next individual enters the PSP

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/21/2015

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate since both individual had a valid background check. However the contractor did not complete the appropriate training for unescorted physical access to a PSP. The [REDACTED] employee that did not have unescorted physical access to the PSP in question is NERC CIP trained and has a current PRA and knows the criticality of working in this environment.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[REDACTED] senior management and direct managers relevant to the situation and the CIP compliance personnel representing the business units involved in the issue actively participated and encouraged employees to provide complete information. Prior to, during, and immediately after the time of the alleged violation, [REDACTED] did not experience any emergencies, security events, or Cyber Security Incidents that directly or indirectly stemmed from the alleged violation.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

Although there are no known system mis-operations, the card reader that is used to validate access was not reset prior to the next person swiping their badge. This provides an opportunity for an individual to "tail gate" on the previous person who does have appropriate access.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Possible Violation (PV) / Find, Fix, and Track (“FFT”) Identification Form

This document is to be completed upon identification of a possible violation (PV), typically within 5 business days of the audit exit brief and emailed to [REDACTED]

For non-FFT candidates: Upon receipt of this document, Enforcement will coordinate with the reporting auditor and Enforcement to initiate the Enforcement processing of this possible violation.

Violation Reported By: [REDACTED]

Submittal Date: [REDACTED]

Candidate for FFT Treatment: YES ☐ NO ☒

Registered Entity: [REDACTED]

NERC Registry ID#: [REDACTED]

Compliance Monitoring Process: Compliance Audits

Standard, Version and Requirement in Violation: CIP-006-3c R1 (R1.6.1)

Registered Function(s) in Violation: [REDACTED]

Initial PV Date (Actual Date Discovered by [REDACTED]): [REDACTED]

Date for Determination of Penalty/Sanction (Beginning Date of Violation): 4/30/2015

End Date of Possible Violation: Unknown

For Non-FFT Candidate ONLY

Violation Risk Factor: VRF - Medium

Violation Severity Level: Moderate VSL

Potential Impact to Bulk Electrical System (BES): Moderate

Provide Explanation for Selection:

[REDACTED] did not provide the required documentation in manual visitor logs for various Physical Security Perimeters.

For Non-FFT and FFT Candidates

Basis for the PV:

The audit team finds a possible violation for CIP-006-3 R1 (R1.6.1). Evidence reviews detected multiple instances of [REDACTED] not documenting the entry and exit of visitors, including the date and time, to and from various Physical Security Perimeters.

Facts and Evidence pertaining to the PV:

Evidence:

- [REDACTED]
- [REDACTED]
- [REDACTED]

Facts:

The audit team reviewed evidence provided for physical access points of the sampled BES assets, request [REDACTED] and [REDACTED]. In this evidence, [REDACTED] had multiple instances of not completing the required information in the manual visitor logs.

The following information was missing within each of the files below.

[REDACTED]

These are the manual Visitor Logs per access point for the PSPs applicable for this audit. Below is the results of our review of the logs.

- pgs 4, 6, 15, 17, 18, 27, 29, 37 - ids were not check
- pg 10 - no dates, no id check, no purpose of visit, no escort, no badge number
- pgs 12, 13, 23, 24, 25 - timeout time
- pgs 18, 20 - use of ditto marks
- pg18 - [REDACTED] filled out the visitor log as the escort
- pg 21 - use '-' in company name
- pgs 26, 29 - no escort badge number
- pg 30 - incomplete date

[REDACTED]

These are the manual Visitor Logs per access point for the PSPs applicable for this audit. Below is the results of our review of the logs.

- pgs7, 32 - missing badge number - internal
- pgs 12 & 19 - missing first name
- pgs 23, 45, 50, 51, 54, 75, 78, 79 - ids were not check
- pgs 24 & 26 - use of dittos
- pgs 29 & 30 & 31, 48 - did not log time-out
- pgs 53, 79 - no legible dates or missing
- pgs 60 - id not check, no in-time and out time
- pgs 66 - no last name
- pgs 77 - no out time, no badge, no first name

[REDACTED]

These are the Visitor Logs per access point for the PSPs applicable for this audit. Below is the results of our review of the logs. These are the same logs that were reviewed under [REDACTED]

Self-Reports:

[REDACTED] also stated they submitted Self-Reports to address some of the issues with the manual visitor logs. The Self-Reports are listed below.

- [REDACTED] Discovered 4/8/15; Occurred 4/7/15
- There are no visitor logs for this issue. The PV occurred because a contractor thought he had authorized unescorted access into a PSP but did not. No log was filed for this issue.

- [REDACTED]
- The logs are contained in [REDACTED] Possible Violation [REDACTED] was rolled into [REDACTED] and will ultimately be addressed in the Mitigation Plan for [REDACTED]

- [REDACTED]
- [REDACTED] Discovered 11/4/2015
 - For August 2015 and September 2015 Logs.
 - The logs are contained in Expansion of Scope PV
 - This Possible Violation will be an expansion of scope for the existing enterprise Mitigation Plan

Open Enforcement Actions:

- [REDACTED]
- Shown under Self-Reports above.

- [REDACTED]
- [REDACTED] Discovered 5/21/15; Occurred 5/21/15
 - Security officer was supposed to escort two different contractor crews. Officer was busy escorting part of crew in another room when a single contractor was discovered unescorted.

- [REDACTED]
- Completed on 4/13/15.

Additional Recommendations:

- Consistently apply Visitor signage to the inside of all Physical Security Perimeter (PSP) Access doors to remind visitors and escorts to sign out of PSPs.
- Also, ensure all manual access log are placed in a location visible to all employees and contractors who enter the PSP.

Summary:

The audit team finds a possible violation for CIP-006-3 R1 (R1.6.1). Evidence reviews detected multiple instances of [REDACTED] not documenting the entry and exit of visitors, including the date and time, to and from various Physical Security Perimeters. Note that the audit scope is for CIP-006-5 R2 (Part 2.2) as part of the CIP Version 5 Transition Program.

For FFT Candidates ONLY

1. Why did this possible violation pose a minimal risk:

[Click here to enter text.](#)

2. Has Registered Entity mitigated this possible violation: YES ☐ NO ☐
- a. If yes, describe mitigating actions and state the date that Registered Entity completed the mitigating actions:

[Click here to enter text.](#)

3. Please answer the following questions to determine whether this possible violation constitutes a “clear on its face” FFT candidate or a “close call.” If the answer to any of the following questions is yes, this possible violation will be treated as a “close call.” Otherwise, this possible violation will be treated as a “clear on its face” FFT candidate.

- A. Is there any disagreement amongst the audit team on whether the PV is a “clear on its face” or “close call” candidate: YES ☐ NO ☐
- a. If yes, explain why:

[Click here to enter text.](#)

- B. Does this possible violation reveal a serious shortcoming in registered entity’s reliability-related processes (e.g. a systematic compliance program failure):

YES ☐ NO ☐

- a. If yes, explain why:



[Click here to enter text.](#)

C. Are there any additional facts the audit team needs to know in order to comfortably designate this possible violation for FFT treatment: YES ☐ NO ☐

a. If yes, state those facts:

[Click here to enter text.](#)

4. Did audit team inform registered entity that this possible violation qualifies for FFT treatment? YES ☐ NO ☐

a. If so, on what date? [Enter Date.](#)

This item was submitted by [REDACTED] on 2/23/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

7/21/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 11/9/2015

Beginning Date of Possible Violation: 11/9/2015

End or Expected End Date of Possible Violation: 11/9/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

Per Requirements listed below: Visitor must have continued escorted access within each PSP. Escort must continuously monitor and keep visual contact of visitor.

CIP006-5- Req 2.1

Visitor must have continued escorted access within each PSP except during CIP emergency circumstances.

Escort has to continually monitor and keep visual contact of Visitor. Visitor can enter a closed room if there is any point of entry and exit.

When: 11/9/15 – around 10:00 am

Where: [REDACTED]

Who: Escort – (Escort)-CW [REDACTED] Visitor #1 (Contractor/Visitor) from [REDACTED] Visitor #2 (Contractor/Visitor) from [REDACTED]

What: Escort duties were not followed for visitor while inside the PSP. Escort did not continuously monitor the entry/exit of the closed room that had one point of entry/exit where Visitor. Escort left the entry/exit of the closed room in order to maintain contact with other visitor.

Misc: The Escort has completed the required NERC CIP PRA and Training.

The nature and number of total devices present at the [REDACTED] were:

[REDACTED] BES Cyber System which contains [REDACTED]

Event: 11/9/15

Project is currently in process for the creation of a new document for the [REDACTED] "Substation operation Information Manual". The scope is large as it requires combining all changes into one document. Two contractors, who are both in the [REDACTED] have been assisting with the creation of this document. This project requires extensive research as the document will consist of operating instructions for everything that operates at the site. It will include such items as OneLine drawings and Floor panels.

That specific day, 11/9/15, the two contractors, arrived at the [REDACTED] to continue work on this project. A safety briefing was done prior to beginning work. Because of the fact that PRAs for the contractors were in process, they did not have badges at that time. This meant that they needed to be treated as visitors and needed an escort.

At one point during the day, approximately 10:00 AM, a break was taken. Visitor #1 went to the restroom and Visitor #2 went to the kitchen to get coffee. The escort, monitored both and saw Visitor #1 go into the restroom. Escort then went to the kitchen with Visitor #2 while coffee was being made. While escort and Visitor #2 were in the kitchen, Visitor #1 had exited the restroom and met escort and Visitor #2 in the kitchen.

An assumption was made by the escort that the act of making the coffee would take a short amount of time and would have been completed before Visitor #1 was finished in the restroom, and escort would have been able to go back to watching the restroom door where Visitor #1 would be exiting. This was an error of judgment but not an intentional error. The escort had watched Visitor #1 enter the restroom and knew that the room had only one point of entry and exit.

Visitor #1 met up with the Escort and Visitor #2 in the kitchen and so both escort and visitors were re-united.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

As soon as Visitor #1 left the restroom, he went directly to the kitchen where escort and Visitor #2 were making coffee. Escort and both visitors were re-united and escort was able to monitor the two visitors for the remainder of the day.

The immediate corrective actions were the reappearance of the visitor in the kitchen following the short absence, as well as continuous monitoring for the rest of the day of the visitors by the escort.

Provide details to prevent recurrence:

Due to the violations that have occurred around the Visitor/Escort events, Transmission engaged the services of a [REDACTED] team member to conduct a Common Cause Analysis. Some of the themes the Analysis identified where improvements are needed:

1. Escort Knowledge of Roles and Responsibilities Lacking
2. Control and Rules Associated with Use of Logs Need Improvement
3. Loss of Control of Large Escorted Groups for Extended Times
4. Lack of Control of Infrequent Contractors
5. What is Tailgating?

A Mitigation Plan has been created to put mitigating activities in place to prevent a recurrence for some of these events. Activities include:

1. A bi-annual communication is being implemented to reinforce the visitor management policy in addition to the information that is found in the annual training. In these communications topics will focus are the areas identified from the cause analysis.
2. Posters are being developed and distributed to all CIP sites to help reinforce the responsibilities.
3. The visitor logs have been redesigned to simplify.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

3/7/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the two visitors, who are contractors, who are both in the [REDACTED] department, had been assisting with the project of the creation of the document, [REDACTED] "operation Information Manual". They had been present in the facility on several other occasions, and had no other incidents of this nature reported for these visitors or this escort.

Also the intent of the escort was not to leave the visitor alone. Escort had monitored Visitor # 1 when he entered the bathroom and was expecting to pick up the monitoring after finishing the activities in the kitchen. Visitor #1 had returned to the kitchen immediately upon leaving the bathroom and did not venture to any other areas while unescorted.

The mitigating actions that took place at the time of the incident was that Visitor #1 went directly to the kitchen upon exiting the bathroom and went straight to the kitchen to join the escort and Visitor #2. The escort continuously monitored the two visitors for the rest of the day.

To prevent occurrence, an alternative action plan was discussed:

Instead of accompanying Visitor #2 into the kitchen, escort would have been able to monitor both the entry/exit door of the bathroom that Visitor #1 went into, and monitor Visitor #2 in the kitchen from the vantage point of the hallway. In this respect, once Visitor #1 emerged from the bathroom, both the escort and Visitor #1 would have been able to join Visitor #2 in the kitchen. This would have prevented Visitor #1 from being left unescorted – even for that short amount of time.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

This item was submitted by [REDACTED] on 4/7/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-006-3c

Applicable Requirement: R1.

Applicable Sub Requirement(s): R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

2/23/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 1/29/2016

Beginning Date of Possible Violation: 1/29/2016

End or Expected End Date of Possible Violation: 1/29/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

In accordance with CIP-006-3c-R1.6.1, [REDACTED] is required to have a visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

The cause of these issues are because [REDACTED] Physical Security Procedure was not followed. Employees and contractors did not correctly fill in all of the entries on the Visitor Log form, and the Escorts did not make sure that all entries were complete on the Visitor Logs. However, the visitors were not left unescorted the entire time they were in the PSP.

Visitor Log entries for December contained possible violations for PSPs in the [REDACTED] regions. These violations occurred in the following fields: "Date", "Escort Name", "Visitor Name", "First Time In", "Last Time Out", and "Escort Badge #".

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

Notice was sent out to each manager, as well as the escorts who had the violations advising them of the violation and the proper procedures that are to be followed. The visitors were not left unescorted the entire time they were in the PSP.

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide details to prevent recurrence:

Due to the violations that have occurred around the Visitor/Escort events, [REDACTED] engaged the services of a [REDACTED] team member to conduct a Common Cause Analysis. Some of the themes the Analysis identified where improvements are needed.

1. Escort Knowledge of Roles and Responsibilities Lacking
2. Control and Rules Associated with Use of Logs Need Improvement
3. Loss of Control of Large Escorted Groups for Extended Times
4. Lack of Control of Infrequent Contractors
5. What is Tailgating?

A Mitigation Plan has been created to put mitigating activities in place to prevent a recurrence for some of these events. Activities include:

1. A bi-annual communication is being implemented to reinforce the visitor management policy in addition to the information that is found in the annual training. In these communications topics will focus are the areas identified from the cause analysis.
2. Posters are being developed and distributed to all CIP sites to help reinforce the responsibilities.
3. The visitor logs have been redesigned to simplify.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

5/1/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the sites being mentioned continue to be secured and monitored on a 24 hour, 7 days a week basis. The visitors were continuously escorted the entire time they were in the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Visitor Log in place at the control center, as well as training, and reviews of Visitor Logs.

An Extent of Condition showed that this condition exists within other groups. As a result of these issues, a Common Cause Analysis was performed and a Mitigation Plan has been developed.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 4/12/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

2/23/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/29/2016

Beginning Date of Possible Violation: 2/29/2016

End or Expected End Date of Possible Violation: 2/29/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]

In accordance with CIP-006-3c-R1.6.1, [REDACTED] is required to have a visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors. The cause of these issues are because [REDACTED] Physical Security Procedure was not followed. Employees and contractors did not correctly fill in all of the entries on the Visitor Log form, and the Escorts did not make sure that all entries were complete on the Visitor Logs. However, the visitors were not left unescorted the entire time they were in the PSP.

Visitor Log entries for January contained possible violations for PSPs in the [REDACTED] region. These violations occurred in the following fields: "First Time In", "Last Time Out".

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

In order to further raise awareness, notice is sent out each month from [REDACTED] to each manager, as well as the escorts who had the violations informing them that they did not follow the procedures.

*See below for an example of the narrative that was sent out by [REDACTED] regarding the visitor logs for the month of January.

=====

"As many of you are aware we have recently rolled out new visitor logs at our NERC CIP protected locations. While we have attempted to provide clear instructions on how to complete these logs we continue to have violations where logs fail to be completed accurately, legibly, or completely. If you are receiving this notification, you or an employee in your organization was recently identified as an escort who did not complete the log correctly and could result in [REDACTED] self-reporting a violation of NERC CIP Requirements. Escorts are responsible for successful and accurate completion of their entries in the visitor log. [REDACTED] is required to review this information with their employees and remind them the importance of completing these logs accurately. [REDACTED] HAS BEEN REDACTED FROM THIS PUBLIC VERSION

To help better illustrate the errors being identified, an excel spreadsheet is attached that has more information and details including a pivot table, error log entries, and charts illustrating errors by business area. You may wish to use the pivot table or sort on your business area (2nd sheet, column O) to more clearly identify the errors in your area. Additionally, several individuals receiving this notification are repeat violators. It is imperative that this be taken seriously or additional corrective actions and discipline may result for continued errors."

Provide details to prevent recurrence:

Due to the violations that have occurred around the Visitor/Escort events, [REDACTED] engaged the services of a [REDACTED] team member to conduct a Common Cause Analysis. Some of the themes the Analysis identified where improvements are needed:

1. Escort Knowledge of Roles and Responsibilities Lacking
2. Control and Rules Associated with Use of Logs Need Improvement
3. Loss of Control of Large Escorted Groups for Extended Times
4. Lack of Control of Infrequent Contractors

A Mitigation Plan has been created to put mitigating activities in place to prevent a recurrence for some of these events. Activities include:

1. A bi-annual communication was implemented to reinforce the visitor management policy in addition to the information that is found in the annual training. In these communications topics will focus on the areas identified from the cause analysis.
2. Posters are being developed and distributed to all CIP sites to help reinforce the responsibilities.
3. The visitor logs have been redesigned to simplify log completion.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

7/1/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the sites being mentioned continue to be secured and monitored on a 24 hour, 7 days a week basis. The visitors were continuously escorted the entire time they were in the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation. Additionally, the visitors were continuously escorted the entire time they were in the PSP.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Visitor Log in place at the control center, as well as training, and reviews of Visitor Logs.

An Extent of Condition showed that this condition exists within other groups. As a result of these issues, a Common Cause Analysis was performed and a Mitigation Plan has been developed

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 6/30/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region:

2/23/2016

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 2/1/2016

Beginning Date of Possible Violation: 1/30/2016

End or Expected End Date of Possible Violation: 4/29/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

In accordance with CIP-006 R1.6.1 [REDACTED] is required to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters (PSP).

On 2/1/2016, a Sr. Security Specialist visited the [REDACTED] Prior to entering the PSP with his badge, he noticed existing visitor log errors and reported them to [REDACTED] The son of an employee had signed in on 1/30/2016; all Visitor Log Fields were not completed.

The visitor was continuously escorted the entire time he was in the PSP.

Upon further investigation, the following facts were identified:

- Maintenance on the door to install a key box caused a disruption to the normal entry and exit of employees with authorized access. All entering/exiting through the door were required to sign the log regardless of authorized access. Having several employees enter through the electronic badging process, logs appear incomplete because employees were required to sign out.
- [REDACTED] was omitted from the listing to receive updates to visitor log data sheet therefore the current form at the door is not the new form that has been distributed from the most recent mitigation plan.

Are Mitigating Activities in progress or completed? Yes

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

1. Meeting to discuss importance of completing manual log emphasized in the [REDACTED] staff meeting
2. Validate with [REDACTED] that [REDACTED] PSP is on the list for update notification

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include the following:

1. Bi-Annual communications have been implemented to reinforce the visitor management policy in addition to the information that is found in the annual training. In these communications, topics will focus on the areas identified from the cause analysis.
2. Posters were developed and distributed to all CIP sites to help reinforce the responsibilities.
3. The visitor logs have been redesigned to simplify.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

4/29/2016

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the site mentioned continues to be secured and monitored on a 24 hour, 7days a week basis.

Provide detailed description of Actual Risk to Bulk Power System:

The visitor was continuously escorted the entire time while in the PSP.

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this alleged violation by having the Visitor Log in place at the control center, as well as training, and reviews of Visitor Logs. An Extent of Condition showed that this condition exists within other groups. As a result of these issues, Root Cause Analysis was performed and Mitigation Plan development is underway.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 8/11/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-006-3c

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

R1.6.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known): [REDACTED]

Date Reported to Region or Discovered by Region: [REDACTED]

8/11/2016

Monitoring Method for previously reported or discovered: [REDACTED]

Self-Report

Has the scope of the Possible Violation expanded: [REDACTED]

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: [REDACTED]

6/3/2016

Beginning Date of Possible Violation: [REDACTED]

6/1/2016

End or Expected End Date of Possible Violation: [REDACTED]

6/1/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED] only.

Per NERC CIP-006-3c R1.6, [REDACTED] is obligated to maintain a visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter) and provide continuous escorted access of visitors within the Physical Security Perimeter.

During a Physical Access Control System (PACS) outage on June 01, 2016, a [REDACTED] contractor without authorized unescorted access was not continuously escorted while in the physical security perimeter at the [REDACTED] which is classified as a [REDACTED]

On June 1, 2016 a Physical Access Control System (PACS) outage occurred throughout the [REDACTED]. This outage stopped the PACS from working but continued to log and allow badge reader access for locally cached personnel. At 5:55pm the Security Guard in charge (SG1) was informed by the [REDACTED] that there was a PACS outage and Alternative Measures were required for NERC CIP locations in their area. SG1 was unable to locate current Alternative Measures guidance. SG1 referred to [REDACTED]. This guidance was outdated and did not require the security guards to remain outside of the PSP and referred to an Emergency Response badge that did not utilize the two factor authentication requirement.

Upon SG1 adhering to the outdated [REDACTED] guidance the SG1 dispatched the roving security guard (SG2) at 6:00pm to the sixth floor of the [REDACTED] in [REDACTED] giving him an Emergency Response Badge. At 6:10 pm SG2 arrived at the elevators on the 6th floor outside of the PSP and informs SG1 of his location. SG1 instructs SG2 to stand guard at the double glass doors outside the PSP. SG1 continued to receive updates from the [REDACTED] and is informed that the PACS is not receiving data, therefore SG1 assumed that the NERC CIP manual (paper) sign in logs are now required for all personnel entering the PSP.

At 6:28pm SG2 asked the [REDACTED] Employee for the location of the Manual Visitor log sheets who then brings SG2 into the [REDACTED] PSP assuming the Emergency Response badge allowed the (SG2) to have authorized access. Once in the PSP, the SOC employee instructs SG2 and the cleaning contractor to sign in using the NERC CIP visitors manual log book without first verifying their access. [REDACTED] Employee leaves SG2 unattended and assigns him as the escort for the cleaning contractor. Unknowing to the [REDACTED] employee, the cleaning contractor has authorized unescorted access to the [REDACTED] and did not require an escort. At the time, SG2 did not have authorized unescorted access to the [REDACTED] and was not authorized to assume escort responsibilities.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

SG1 observes on the camera (CCTV) that the SG2 was inside of the [REDACTED] PSP and instructs him to exit the PSP and post outside of the PSP. SG2 informs him that he was instructed to escort the cleaning contractor and continued to do so until the cleaning person was finished, then SG2 cleared his post at 8:55pm. [REDACTED] employee did not provide continuous escorting of the visitor SG2. The [REDACTED] Employee was listed as the escort of SG2 in the visitor log book.

On June 2, 2016 @ 2:22pm [REDACTED] was informed of the Potential Violation by the [REDACTED]. [REDACTED] took lead on the investigation and determined that the roving guard (SG2) did not have authorized unescorted NERC CIP access to the [REDACTED] PSP. Further investigation also determined that the cleaning person that initially was being escorted by the roving security guard (SG2) has completed required annual NERC CIP training, PRA qualifications and has authorized unescorted NERC CIP access to the [REDACTED] PSP. Although the cleaning personnel was authorized as an escort and was continuously with the SG2, clear escorting responsibilities were not understood by the cleaning personnel during this incident.

The cause of this incident is lack of or awareness to recent procedural changes for both the security guards and the [REDACTED] employee's alternative measures responsibilities.

Sites in scope:

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken or plans to take with respect to this issue include the following:

- ? [REDACTED] will ensure the distribution of Alternative Measures to Security Operations Personnel
- ? [REDACTED] will provide the [REDACTED] Personnel with the Alternative Measures Process
- ? *An Operator Desk Guide will be created that will summarize the alternative measures that affect the System Operators
- ? *The Operator and staff will be trained on Alternative Measures Operator Desk Guide

Provide details to prevent recurrence:

Due to the violations that have occurred around the Visitor/Escort events, a new root cause is being performed to identify additional actions to help prevent recurrence in addition to the previously implemented items

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

6/15/2017

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the sites being mentioned continue to be secured and monitored on a 24 hour, 7 days a week basis. The visitors were in the presence of a trained and screened person even though that person didn't realize he was acting as an escort the entire time the security guard was in the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation. Additionally, the visitors was with a trained and screened person the entire time they were in the PSP.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Visitor Log in place at the control center, as well as training, and reviews of Visitor Logs.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 19

Record documents for the violation of CIP-006-6 R1

19.a The Companies' Self-Report [REDACTED]

19.b The Companies' Self-Report [REDACTED]

19.c The Companies' Self-Report [REDACTED]

19.d The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 2/9/2018

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-006-6

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

1.1.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 11/29/2017

Beginning Date of Possible Violation: 11/29/2017

End or Expected End Date of Possible Violation: 11/29/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

In accordance with NERC CIP006-6 R1.1, [REDACTED] is required to define operational or procedural controls to restrict physical access. On November 29, 2017, a [REDACTED] badged office supplies vendor piggybacked into the [REDACTED] on an authorized [REDACTED] employee's exit, therefore [REDACTED] is in possible violation of CIP006-6 R1.1.

At 16:28 on November 29, 2017, a [REDACTED] office supplies vendor, badged for general building access (but not for PSP space), entered the 2nd floor of the [REDACTED] facility with a package delivery for an employee located within the Physical Security Perimeter (PSP). The vendor was a new delivery person for the [REDACTED] account and this was his first time servicing the facility on his own.

Upon arrival at the PSP entrance (16:30:47), the vendor was unsure how to deliver the package beyond the locked door.

At 16:31:28, a [REDACTED] employee exited the PSP and did not secure the door upon exit. The office supplies vendor entered the PSP before the door shut (piggybacking) at (16:31:31).

A Security Officer posted near the PSP observed the vendor entering the PSP space without the proper authorization and immediately contacted his management. Upon notification, the Shift Supervisor promptly responded to the call on the 2nd floor.

The office supplies vendor entered the PSP to deliver the package. Two [REDACTED] Employees were in the hallway and engaged the delivery vendor, took the package, and the vendor was followed out of the PSP.

At 16:33:36, the vendor exited the PSP. The Security Officer engaged the vendor requesting him to wait for the Shift Supervisor.

At 16:34, the Shift Supervisor arrived at the 2nd Floor Security Officer's Post and discussed the incident with the vendor to gather further information about the situation. [REDACTED] management informed the vendor about the security of the area and directed him to leave packages outside the entrance of the PSP in the future.

Upon discovery of the incident, [REDACTED] Security management made notifications to appropriate staff and management within [REDACTED]. The [REDACTED] team conducted a thorough review of the video footage. After review and discussions between all parties involved, [REDACTED] determined that the entry by the office supplies vendor into the PSP did not have malicious intent. Therefore [REDACTED] did not initiate the [REDACTED]

During the period of time the office supplies vendor was in the hallway within the PSP (a total of 2 minutes/4 seconds), at no time did he have direct access to any BES Cyber Assets. [REDACTED] BES Cyber Assets are contained within additional layers of security inside the PSP. Video footage specifically captured the vendor time of entry into the PSP (16:31:32) and exit from the PSP (16:33:36).

This entire incident was less than 4 minutes in length.

Nature and Number of Devices Involved

[REDACTED]

The mitigating activities that [REDACTED] has taken with respect to this issue include the following:

[REDACTED] removed the access privileges for the office supplies vendor and provided training to the vendor management and the individual. [REDACTED] reinstated access privileges to the vendor after completion of the training.

[REDACTED] issued an email to all persons with NERC CIP physical access to provide information on the incident. This email also provided a video of the incident along with an example of how to properly secure a door upon exit.

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Electric System was minimal because this PSP access point was monitored by human observation, and as soon as the incident occurred, immediate actions were taken by employees to resolve the issue. [REDACTED] BES Cyber Assets are contained within another layer of security within the PSP – the vendor did not have access to these areas. The vendor was badged to conduct deliveries for [REDACTED] within the "general" areas of the company. Employees within the PSP were observant and when they noticed someone out of the ordinary, they immediately engaged the individual.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Electric System caused by this alleged violation because there were no mis-operations, emergencies, or other adverse consequences to the Bulk Electric System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

[REDACTED] senior management and direct managers relevant to the incident actively participated and encouraged employees to provide complete and accurate information.

There were no extenuating circumstances with respect to the cause of the possible violation. The possible violation took place on a day with normal operations – this did not occur while an Energy Emergency was in effect.

[REDACTED] conducted an Enterprise Extent of Condition (EOC) with its Business Areas. The survey focused on tailgating controls and training. All groups adhere to the requirement to complete the [REDACTED] training prior to granting access and refresher training on an annual basis. The EOC revealed no other reported instances of tailgating at a PSP.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/8/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-006-6

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

1.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 8/10/2016

Beginning Date of Possible Violation: 7/1/2016

End or Expected End Date of Possible Violation: 8/12/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]
Per CIP-006-6 R1.2, [REDACTED] shall utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access. On 08/10/2016 [REDACTED] discovered that a "general" physical access category was not removed from a NERC CIP Physical Security Perimeter (PSP), thus, [REDACTED] in possible violation of CIP-006-6 R1.2.

On 08/10/2016, [REDACTED] discovered an improper access category assigned to the [REDACTED] which is a [REDACTED]. This was discovered during preparation of access categories for a future NERC CIP site.

The site had the improper access category of [REDACTED] as well as the proper NERC CIP category [REDACTED] programmed. Upon discovery, [REDACTED] removed the [REDACTED] category from [REDACTED] on 08/10/2016.

On 08/12/2016 conducted an Extent of Condition and results indicated that [REDACTED] locations were also programmed with the same general physical access category. These PSP locations were identified as [REDACTED] and [REDACTED].


[REDACTED] removed the [REDACTED] category from both [REDACTED] confirmed that the access categories for [REDACTED] had not changed since 07/01/2016 until the removal of the [REDACTED] category.

On 08/12/2016, [REDACTED] reviewed [REDACTED] history reports from the Physical Access Control System (PACS) for the [REDACTED] with the [REDACTED] category. The results revealed that one (1) employee with the [REDACTED] category entered the [REDACTED] on 7/13/2016. The employee was not authorized for the [REDACTED] access category. In addition, the employee did not have a current [REDACTED] and had not completed the [REDACTED] training. There were no other instances of an access attempt with the [REDACTED] category for any of the [REDACTED] locations between 7/1/2016 and 8/12/2016.

[REDACTED] conducted a review of access categories for all [REDACTED] locations and confirmed that locations were correctly programmed with the appropriate NERC CIP access category and did not have the general access category assigned.

The initial cause analysis indicates this possible violation is a human performance issue. [REDACTED] contracted employees performed operability testing during site commissionings and failed to remove the general access category.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

On 8/10/2016, [REDACTED] removed the [REDACTED] category from the [REDACTED]

On 8/12/2016, [REDACTED] removed the [REDACTED] from the [REDACTED]

Provide details to prevent recurrence:

[REDACTED] is performing an Apparent Cause Analysis (ACA) to determine the primary and associated causes of this incident. Corrective actions will be determined as an outcome of this review.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/12/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Moderate

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is moderate because the general access category that was not removed to the [REDACTED] locations may have allowed a [REDACTED] employee or contractor without a NERC CIP Personal Risk Assessment (PRA) and/or the required NERC CIP training to gain access to the facility.

Immediately upon discovery [REDACTED] removed the general access category from all [REDACTED]

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

This alleged violation was not the result of intentional action to violate a NERC reliability standard.

[REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant alleged violation situation.

[REDACTED] relevant to the situation actively participated and encouraged employees to provide complete information.

There were no extenuating circumstances existed with respect to the cause of the alleged violation.

[REDACTED] conducted an Extent of Condition to determine if any other NERC CIP locations had the general access category assigned to them. The results indicated that [REDACTED] additional NERC CIP locations had the general access category assigned. [REDACTED] removed the general access category from all affected locations. In addition, a review was conducted of the valid access records to determine if anyone without the proper NERC CIP access category entered any of the [REDACTED] PSPs in question. The results concluded only one (1) individual entered with the general access category on 07/13/2016.

identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

This item was submitted by [REDACTED] on 5/26/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: [REDACTED]

CIP-006-6

Applicable Requirement: [REDACTED]

R1.

Applicable Sub Requirement(s): [REDACTED]

1.4.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 5/1/2017

Beginning Date of Possible Violation: 4/28/2017

End or Expected End Date of Possible Violation: 5/1/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This self-report applies to [REDACTED]

On Thursday, April 20th, [REDACTED] conducted an activity to clear non-regulated alarms from the Physical Access Control System (PACS).

A report was generated for this activity and was incorrectly filtered and included a regulated alarm point that was inadvertently disabled. Below are the details related to the specific access point disablement:

At 1:51 PM on Friday, April 28th, [REDACTED] Specialists (PACS Administrators) incorrectly disabled the alarming and monitoring for an exit-only door at the [REDACTED]

At approximately 11:00 AM on Monday, May 1st, 2017 a [REDACTED] Specialist was completing change documentation and discovered that the alarming and monitoring at [REDACTED] was disabled. At 11:13 AM, the PACS Administrator re-enabled alarming and monitoring on this door. In addition, at 12:45 PM the [REDACTED] Specialist worked with [REDACTED] to perform local alarming and monitoring operability testing and inspect for physical tampering. Alarming and monitoring tested successfully and no signs of physical tampering were discovered.

The NERC access point did not have alarming and monitoring for a total of 2 days, 21 hours, 22 minutes (From 1:51 PM on Friday, April 28th, 2017 to 11:13 AM on Monday, May 1st, 2017).

[REDACTED] is a [REDACTED] located in [REDACTED]

[REDACTED] contains the following assets:

[REDACTED]

Are Mitigating Activities in progress or completed? No

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Power System is minimal because

Alarming and Monitoring for [REDACTED] was re-enabled after 2 days, 21 hours, 22 minutes, operability and testing was successfully performed, physical inspection on this door resulted in no signs of breach or tampering, [REDACTED] management conducted a stand down meeting to ensure no other alarms were disabled, and video footage associated with motion detection in the area at this door was reviewed and the door was not opened during the absence of alarming and monitoring.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because the access point was secure and there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard. [REDACTED] was attempting to comply in good faith with the applicable NERC reliability standard at issue in this instant possible violation situation. Direct managers relevant to this situation actively participated the moment they were made aware of it and encouraged employees to provide complete information. There were no misoperations, system operating limits, or interconnection reliability operating limits during the course of the potential noncompliance time period.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/2/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard:

CIP-006-6

Applicable Requirement:

R1.

Applicable Sub Requirement(s):

1.8.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 8/11/2016

Beginning Date of Possible Violation: 8/11/2016

End or Expected End Date of Possible Violation: 8/11/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

Applies to [REDACTED]
Per NERC CIP 006-6 R1.8, [REDACTED] is obligated to log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.

Per [REDACTED] policy, a [REDACTED] employee with a forgotten badge must be treated as a visitor. This includes logging in and out of a PSP using the manual log. An employee with authorized unescorted access forgot his badge and was escorted into the Physical Security Perimeter without signing in or out of the visitor log on Thursday August 11, 2016.

Six [REDACTED] employees were involved in the actual incident but only one employee failed to sign the visitor log book.

Time line of incident:

- 9:45am [REDACTED] enter into the [REDACTED]
- 9:48am [REDACTED] leave to hold meeting at a larger location
- [REDACTED] employee failed to complete NERC CIP Visitor log book

The violation was reported by one of the [REDACTED] Employees that attended the meeting.

Event Details:

There was a meeting scheduled by [REDACTED] at [REDACTED] on 8/11/2016 to discuss upcoming fall outages. At approximately 9:45am [REDACTED] employees entered into the [REDACTED] and immediately realized the scheduled location was not large enough to accommodate all attendees; after that realization they all immediately exited the location then proceeded with the meeting in a nearby job trailer. Among the attendees was a [REDACTED] employee that has Authorized NERC CIP access but failed to bring the employee badge to work, the employee did not log in and out of the NERC CIP Visitor Log Book therefore the employees entrance into the Physical Security Perimeter (PSP) was not documented.


The Extent of Condition document which was submitted on 8/26/16 to other business units shows those other business units did not have the same Potential Violation.

[REDACTED] does not have a preventative control in the situation in which multiple people are entering a PSP and one of the individuals has a forgotten badge and needs to sign-in. Controls such as signage, training, monitoring of visitor logs, and communication to business areas of violations exist to try to reduce this risk.

Site in scope:

[REDACTED]

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has with respect to this issue include the following:

*The visitor log book entry requirement for employees who have forgotten their badge was discussed with employee who did not sign the visitor log book.

Provide details to prevent recurrence:

Due to the violations that have occurred around the Visitor/Escort events, a new root cause is being performed to identify additional actions to help prevent recurrence in addition to the previously implemented items.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/30/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The Potential Impact to the Bulk Power System is minimal because the sites being mentioned continue to be secured and monitored on a 24 hour, 7 days a week basis. The visitors were continuously escorted the entire time they were in the PSP.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this possible violation. Additionally, the visitors were continuously escorted the entire time they were in the PSP.

Additional Comments:

[REDACTED] was attempting to comply in good faith with the application NERC reliability standard at issue in this instant alleged violation situation by having the Visitor Log in place at the [REDACTED] as well as training, and reviews of Visitor Logs.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 20

Record documents for the violation of CIP-006-3c R2.2

20.a The Companies' Self-Report

20.b The Companies' Self-Report

This item was submitted by [REDACTED] on 7/23/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

R2.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

10/23/2013

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 4/1/2015

Beginning Date of Possible Violation: 12/31/2014

End or Expected End Date of Possible Violation: 8/31/2015

Is the violation still occurring? Yes

Provide detailed description and cause of Possible Violation:

Per CIP-006-3 R2.2, all PACs devices must adhere to the requirements in CIP007-3. CIP-007-3 R5.1.3 requires that EACMs must adhere to annual review for CIP-003-3 R5. CIP-003-3 R5.2 requires that:

[REDACTED] is in the process of implementing a new Identity Access Management tool that will assist in identifying critical cyber assets, accounts on those assets and the people who have access to those assets and accounts.

During discussions on the implementation of the new tool a question arose as to why PAC's (T3 critical assets) were not included in the [REDACTED] review.

On April 1, 2015 the IT CIP Lead realized the [REDACTED] managed PAC's were not included in the CIP007-3 R5 Annual Account Management Review.

Attached are the identified PAC's (Tier3) identified in the [REDACTED] region that were omitted from the Annual 2014 CIP007-3 R5 Account Management review.

There are [REDACTED] PAC's located in the [REDACTED] region. They are identified as [REDACTED] These assets are located at the [REDACTED]

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitigating Activities:

The PAC's have been identified and a review of the assets, applicable accounts and people who have access to those PAC's and accounts is in progress.

Anticipated completion date: 8/31/2015

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Provide details to prevent recurrence:

The actions that [REDACTED] is taking to prevent recurrence include:

Reviewing the current process for identifying all assets to be included in the CIP007-3 R5 Account Management Annual review to ensure EACM's are not missed in future reviews.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

8/31/2015

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

The potential impact to the Bulk Electric System is minimal because the same individuals who have access to the identified PAC's also have access the Critical Cyber Assets that were included in the 2014 CIP007-3 R5 Access Management annual review and no unauthorized individuals were identified as having access to the Critical Cyber Assets in the 2014 CIP007-3 R5 Access Management annual review.

A review of the identified PAC's is currently underway and is anticipated to be completed by 8/31/2015.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this alleged violation because there were no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of this alleged violation.

Additional Comments:

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 10/29/2015

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-006-3c

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

R2.2.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

2/23/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: Yes

If yes, indicate which Region(s):

Date Reported to Region(s):

5/13/2015

Date Possible Violation was discovered: 5/20/2015

Beginning Date of Possible Violation: 5/20/2015

End or Expected End Date of Possible Violation: 5/20/2015

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

During Q2 access review it was determined that access lists were not updated with changes within 7 calendar days for PAC Servers. During this period a user account was removed from 2 PAC Servers. Notification of account removal was not properly documented; subsequent update to access list was not performed within required timeframe. In addition, a user account was provisioned for access to the same 2 PAC Servers. Notification of account provisioning was not properly documented; subsequent update to access list was not performed within required timeframe.

Causes for discrepancies due to manual maintenance processes of independent access lists.

Are Mitigating Activities in progress or completed? Yes

As of June 9, 2015 the [REDACTED] HR system was updated adding a CIP flag to HR records for personnel with access to CIP assets. Changes to personnel with access to CIP assets generate alerts assisting administrators in maintaining accurate authorization records. Independent access lists [REDACTED] **PRIVATE AND CONFIDENTIAL INFORMATION** system generated alerts are utilized for maintaining accurate accounting of CIP access.

lists are no longer used. As of August 31, 2015

**PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

Mitigation Plan minimizes probability of further issues with quarterly access reviews. The actions performed in this mitigation plan remove manual maintenance processes of independent lists, which have been problematic. The Mitigation Plan assists in ensuring future personnel changes are recorded in an accurate and timely manner.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

Attachment 21

Record documents for the violation of CIP-006-6 R2

21.a The Companies' Self-Report [REDACTED]

21.b The Companies' Self-Report [REDACTED]

21.c Audit Summary [REDACTED]

21.d The Companies' Self-Report [REDACTED]

21.e The Companies' Self-Report [REDACTED]

21.f The Companies' Self-Report [REDACTED]

21.g The Companies' Self-Report [REDACTED]

21.h The Companies' Self-Report [REDACTED]

This item was submitted by [REDACTED] on 9/12/2017

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity:

NERC Registry ID:

JRO ID:

CFR ID:

Entity Contact Information:

REPORTING INFORMATION

Applicable Standard:

CIP-006-6

Applicable Requirement:

R2.

Applicable Sub Requirement(s):

2.1.

Applicable Functions:

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

Date Reported to Region or Discovered by Region:

5/22/2017

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

No

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 11/17/2016

Beginning Date of Possible Violation: 8/8/2016

End or Expected End Date of Possible Violation: 8/8/2016


Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On August 8, 2016, a [REDACTED] custodial contractor with authorized unescorted access to the PSP was escorting an unauthorized custodial contractor (visitor) in the [REDACTED] to perform janitorial services.

At 10:40am the custodial contractor observed a spill on the break room floor and left the PSP to retrieve a mop bucket from outside the PSP and left the visitor unescorted until 10:41 (one minute). The escort required the visitor to remain at the site of the spill to alert and avoid against slips, trips and other safety hazards. At 10:41am the escort returned to the PSP to ensure the safety hazard was cleared. During this one-minute period, the visitor was left unescorted resulting in a possible violation of the above referenced standard and requirement.

Are Mitigating Activities in progress or completed? Yes

 An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating activities. If you would like to formalize that Mitigation Plan, please contact the Region.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitigating Activities:

The mitigating activities that [REDACTED] has taken with respect to this issue include:

- [REDACTED] no longer allows contractors to act as escorts; only [REDACTED] technicians can perform escort responsibilities. This was formalized in the [REDACTED]
- All [REDACTED] employees and contractors were trained on the new [REDACTED]
- All custodial contractors who enter PSPs to perform janitorial work are now badged.

Provide details to prevent recurrence:

Only [REDACTED] employees [REDACTED] technicians can now act as escorts for visitors; this keeps the responsibility with a trained group who performs these duties frequently, and who are familiar with the proper procedures. Annual training on the [REDACTED] is required.

Date Mitigating Activities (including activities to prevent recurrence) are expected to be completed or were completed:

11/14/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
No data available in table			

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

Provide detailed description of Potential Risk to Bulk Power System:

Potential impact to the Bulk Power System is minimal because the period the visitor was left unescorted was 1 minute. After discovery of the incident, escort responsibilities were removed from third party contractors.

Provide detailed description of Actual Risk to Bulk Power System:

There was no Actual Impact to the Bulk Power System caused by this possible violation because there was no misoperations, emergencies, or other adverse consequences to the Bulk Power System as a result of the possible violation.

Additional Comments:

This possible violation was not the result of intentional action to violate a NERC reliability standard.

NOTE: While submittal of a mitigation plan is not required until after a determination of a violation is confirmed, early submittal of a mitigation plan to address and remedy an identified deficiency is encouraged. Submittal of a mitigation plan shall not be deemed an admission of a violation. (See NERC Rules of Procedure, Appendix 4C, Section 6.4.)

This item was submitted by [REDACTED] on 9/2/2016

Please note that the circumstances under which an Entity would submit a Scope Expansion form are different from what would require a new Self-Report. Please review the material in [this link](#) to see clarifying information and examples of these differences before continuing with this form.

FORM INFORMATION

Registered Entity: [REDACTED]

NERC Registry ID: [REDACTED]

JRO ID: [REDACTED]

CFR ID: [REDACTED]

Entity Contact Information: [REDACTED]

REPORTING INFORMATION

Applicable Standard: CIP-006-6

Applicable Requirement: R2.

Applicable Sub Requirement(s): 2.2.

Applicable Functions: [REDACTED]

Has a Possible violation of this standard and requirement previously been reported or discovered: Yes

If yes, provide NERC Violation ID (if known):

[REDACTED]

Date Reported to Region or Discovered by Region:

6/21/2015

Monitoring Method for previously reported or discovered:

Self-Report

Has the scope of the Possible Violation expanded:

Yes

Has this Possible Violation previously been reported to other Regions: No

Date Possible Violation was discovered: 8/8/2016

Beginning Date of Possible Violation: 8/8/2016

End or Expected End Date of Possible Violation: 8/8/2016

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

This applies to [REDACTED]
Visitors were escorted into the Physical Security Perimeter without signing in or out on the visitor log on Monday August 8, 2016 therefore [REDACTED] is out of compliance with CIP-006-5 R2.2

At approximately 11:15 am on August 8, 2016 a contractor was escorting two of his executives from his company to present the completed work in the 2nd floor of the [REDACTED]. The group entered into the Northeast door of the [REDACTED] after the contractor badged and keyed in his access number. Upon entering into the [REDACTED] the contractor questioned the [REDACTED] on the location of the visitor logbook that was previously located on the file cabinet upon commissioning the [REDACTED]. The Operator explained to the contractor that the log book was moved, and is now located at the outside of the West door and if they don't have NERC CIP Access they have to leave. Contractor explained to the Operators that he does have authorized access but felt it was best to leave the [REDACTED] at that point with the construction executives.

The violation was reported by the hiring manager.

Event Details:

Time line of incident:

? 11:15 AM Contractor enters [REDACTED] with the construction executives
? Executives remain at the Physical Security Perimeter door entrance waiting for the contractor to locate the log book
? Contractor approaches the [REDACTED] for help locating the logbook
? Contractor is informed by the Operators that the logbook is now located outside the west door
? 11:20 AM the Contractor turns and immediately leaves the [REDACTED] with the executives through the east door