June 27, 2019

VIA ELECTRONIC FILING

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

Re: **NERC Full Notice of Penalty regarding [redacted]**
the FERC Docket No. NP19- -000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by [redacted] the Entities), NERC Registry ID numbers [redacted] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[4] with the Commission because SERC Reliability Corporation (SERC) and the Entities have

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation,* Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2017). *Mandatory Reliability Standards for the Bulk-Power System,* FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied,* 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] [redacted]

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[4] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations of the CIP Reliability Standards listed below.

According to the Settlement Agreement, the Entities admit to the violations and have agreed to the assessed penalty of seven hundred and seventy-five thousand dollars ($775,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SERC and the Entities. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2019), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req.	VRF/VSL	Applicable Function(s)	Discovery Method* Date	Violation Start-End Date	Risk	Penalty Amount
SERC2016015954	CIP-002-5.1	R1	High/ Lower	[redacted]	SR 7/25/2016	7/1/2016- 9/7/2017	Moderate	$775,000
SERC2017018136	CIP-004-6	R5	Medium/ High	[redacted]	SR 8/7/2017	5/2/2017- 6/10/2017	Moderate	
SERC2017018279	CIP-004-6	R5	Medium/ Moderate	[redacted]	SR 8/29/2017	11/6/2016- 6/29/2017	Moderate	
SERC2017018774	CIP-005-5	R1	Medium/ Severe	[redacted]	SR 12/12/2017	9/12/2017- 9/12/2017	Minimal	
SERC2016016548	CIP-005-5	R2	Medium/ Moderate	[redacted]	SR 11/18/2016	7/1/2016- 8/10/2016	Serious	
SERC2017017286	CIP-006-6	R1	Medium/ Severe	[redacted]	SR 3/24/2017	12/5/2016- 1/31/2017	Moderate	
SERC2017018440	CIP-006-6	R2	Medium/ Severe	[redacted]	SR 10/6/2017	2/1/2017- 6/7/2017	Moderate	
SERC2017018441	CIP-006-6	R2	Medium/ Severe	[redacted]	SR 10/6/2017	4/20/2017- 1/22/2018	Moderate	
SERC2016016492	CIP-007-6	R1	Medium/ High	[redacted]	SR 11/3/2016	7/1/2016- 8/2/2016	Minimal	
SERC2017018467	CIP-007-6	R2	Medium/ Moderate	[redacted]	SR 10/11/2017	8/15/2017- 9/8/2017	Moderate	
SERC2017017236	CIP-007-6	R3	Medium/ Severe	[redacted]	SR 3/16/2017	10/2/2016- 2/7/2017	Moderate	
SERC2017016832	CIP-007-3a	R5	Medium/ Severe	[redacted]	SR 1/25/2017	5/31/2011- 11/22/2016	Serious	
SERC2017018246	CIP-007-6	R5	Medium/ Severe	[redacted]	SR 8/24/2017	7/1/2016- 8/15/2017	Moderate	

SERC2018019200	CIP-007-6	R5	Medium/ Severe	[redacted]	SR 2/16/2018	7/1/2016-1/8/2018	Moderate	$775,000
SERC2017018548	CIP-007-6	R5	Medium / Severe	[redacted]	SR 10/30/2017	5/25/2017-6/13/2017	Minimal	
SERC2016016339	CIP-007-6	R5	Medium/ High	[redacted]	SR 10/6/2016	7/1/2016-8/25/2016	Minimal	
SERC2016016321	CIP-010-2	R1	Medium/ Lower	[redacted]	SR 9/30/2016	7/1/2016-6/22/2017	Serious	
SERC2018019106	CIP-010-2	R1	Medium/ Severe	[redacted]	SR 2/2/2018	11/18/2016-10/12/2017	Moderate	
SERC2016016379	CIP-011-2	R1	Medium/ Severe	[redacted]	SR 10/19/2016	7/1/2016-7/29/2016	Minimal	
SERC2016016572	CIP-011-2	R1	Medium/ Severe	[redacted]	SR 11/28/2016	7/1/2016-9/29/2016	Moderate	
SERC2017017564	CIP-011-2	R1	Medium/ Severe	[redacted]	SR 5/15/2017	7/1/2016-8/13/2018	Moderate	

Background to the Violations

[redacted]

The Entities and SERC entered into a Settlement Agreement to resolve 21 violations of the CIP Reliability Standards. The Entities self-reported all violations. The violations discussed herein are a result of The Entities' adjustment to CIP Version 5. CIP Version 5 involved a major expansion of scope for some of The Entities' business units that were still new to CIP compliance. The Entities were formalizing a CIP internal controls program when the CIP Version 5 Standards became effective. Because supporting controls and training were not in place, The Entities applied their CIP procedures inconsistently. Nonetheless, The Entities discovered the noncompliance and submitted Self-Reports and mitigation in a timely manner to SERC, demonstrating their strong culture and commitment to security and compliance.

CIP-002-5.1 R1

SERC2016015954

SERC determined that The Entities did not properly classify [redacted] medium impact BES Cyber Systems (BCSs) by the CIP Version 5 effective date of July 1, 2016. [redacted]

The cause of this violation was insufficient management oversight in planning and failure in the implementation of the transition to CIP Version 5.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 2a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachment 2b includes a description of the mitigation activities The Entities took to address this violation. A copy of the Mitigation Plan is included as Attachment 2b.

The Entities certified that they had completed all mitigating activities. Attachment 2c provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-004-6 R5

SERC determined that The Entities were in noncompliance with CIP-004-6 R5 in two separate violations.

SERC2017018136

SERC determined that The Entities did not, in two separate instances, initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and failed to complete the removals within 24 hours of the termination.

The root cause of the violation was insufficient training in access revocation procedures.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 3b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 3b provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2017018279

SERC determined that The Entities did not revoke an individual's authorized electronic access to individual accounts by the end of the next calendar date following the date that The Entities determined that the individual no longer required electronic access. As a result, the employee retained access to one EMS data center, [redacted]

The root cause of the violation was a lack of detailed procedures regarding access removal, and a lack of emphasis on training regarding quarterly access reviews.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 3c includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 3d include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 3d provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-005-5 R1

SERC2017018774

SERC determined that The Entities did not ensure an applicable Cyber Asset was connected to a network via a routable protocol, which resided within a defined Electronic Security Perimeter (ESP).

The root cause of the first violation was an insufficiently granular fieldwork procedure for removing devices from within ESPs, and inadequate training for carrying out these activities.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 4a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 4b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 4b provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-005-5 R2

SERC2016016548

SERC determined that The Entities allowed IRA to BCSs without using an Intermediate System. Upon investigation, The Entities found that three employees had been able to bypass the IRA Intermediate System from outside an ESP.

The root cause of this violation was an oversight in the documented procedures related to utilizing the IRA Intermediate System. Specifically, The Entities did not guard against using the port to bypass the IRA Intermediate System because it implemented the port for a different purpose.

SERC determined that this violation posed a serious risk to the reliability of the bulk power system (BPS). Attachment 5a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 5b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 5c provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-006-6 R1

SERC2017017286

SERC determined that The Entities did not use at least one physical access control to limit unescorted physical access into each applicable Physical Security Perimeter (PSP) to only individuals who have authorized unescorted physical access. The Entities did not update a CIP Physical Access Control System (PACS) employee badge to remove permissions when an employee reported that they had lost their badge.

The root cause of this violation was a lack of training for the employee that issued the replacement badge. Additionally, there was a lack of internal controls governing badge management and badge assignment.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 6a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 6b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 6c provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-006-6 R2

SERC determined that The Entities were in noncompliance with CIP-006-6 R2 in two separate violations.

SERC2017018440

SERC determined that The Entities did not continuously escort a visitor while inside a PSP in one instance, and did not document all required information in their logbooks for visitors who accessed The Entities' PSPs in four different instances.

The root cause of this violation was insufficient training related to the visitor control program.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 7a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 7b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 7b provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2017018441

SERC determined that The Entities did not continuously escort visitors while inside PSPs in three different instances, and did not document all required information in its logbooks for visitors who access The Entities' PSPs in two different instances.

The root cause was insufficient training related to the visitor control program.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 7c includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 7d include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 7d provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-007-6 R1

SERC2016016492

SERC determined that The Entities enabled two logical network accessible ports when The Entities no longer needed them.

The root cause of this violation was insufficient training to ensure the successful execution of commissioning-related procedures for disabling ports The Entities no longer needed.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 8a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 8b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 8b provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-007-6 R2

SERC2017018467

SERC determined that in one instance The Entities did not deploy an applicable patch onto two Electronic Access Control or Monitoring Systems (EACMS) servers containing medium impact BES Cyber Systems within 35 calendar days of completion of the patch evaluation. The missed patch addressed security vulnerabilities, security updates, or unsupported hardware not being scanned for, and issues with printing and using a mouse.

The root cause of this violation was deficient procedures that lacked details related to roles and responsibilities, as well as related internal controls.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 9a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 9b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 9b provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-007-6 R3

SERC2017017236

SERC determined that in one instance The Entities did not deploy a method to deter, detect, or prevent malicious code. A process to enforce whitelisting stopped working properly on [redacted] EACMS servers. The Entities used the method of whitelisting to deter, detect, or prevent malicious code.

The root cause of this violation was faulty software that caused the process to stop working.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Attachment 10a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 10b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 10c provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-007-3a R5

SERC2017016832

SERC determined that The Entities did not change passwords for [redacted] Critical Cyber Asset (CCA) Servers prior to commissioning them into service, and did not change passwords for such accounts annually thereafter. The Entities did not change the passwords on the [redacted] CCAs for nearly five years.

The root cause of this violation was a lack of adequate training and internal controls that failed to ensure the proper documentation of server inventory and password status.

SERC determined that this violation posed a serious risk to the reliability of the bulk power system (BPS). Attachment 11a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 11b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 11c provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-007-6 R5

SERC determined that The Entities were in noncompliance with CIP-007-6 R5 in four separate violations.

SERC2017018246

SERC determined that in two instances The Entities did not authenticate interactive user access to PACS Cyber Assets where technically feasible. In total, The Entities' employees mistakenly added unauthorized domain groups to [redacted] PACS workstations, allowing unauthorized users to have remote access to the workstations.

The root cause of this violation was a lack of managerial oversight, a lack of internal controls, and inadequate training on properly implementing internal controls.

SERC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Attachment 12a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 12b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 12c provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2018019200

SERC determined that The Entities did not change known default passwords, per Cyber Asset capability, for [redacted] EACMS servers. Additionally, The Entities did not identify and inventory all known enabled default generic account types for two of the servers.

The root cause of this violation was incomplete and insufficient procedures related to the deployment of newly commissioned Cyber Assets.

SERC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Attachment 12d includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 12e include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 12f provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2017018548

SERC determined that The Entities did not change known default passwords for two accounts on a Remote Terminal Unit when it commissioned the device.

The root cause of this violation was a lack of adequate training in commissioning procedures.

SERC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. Attachment 12g includes the facts regarding the violations that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 12h include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 12h provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2016016339

SERC determined that in one instance The Entities did not implement a password length of at least eight characters for an interactive user access account. The deficient password length setting applied to the Cyber Assets and their associated EACMS and PACS.

The root cause of this violation was a lack of adequate training on procedures for password requirements.

SERC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. Attachment 12i includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 12j include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 12j provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-010-2 R1

SERC determined that The Entities were in noncompliance with CIP-010-2 R1 in two separate violations.

SERC2016016321

SERC determined that in 15 instances The Entities did not properly implement documented processes for baseline configuration change management when transitioning from CIP Version 3 to CIP Version 5. This included developing baseline configurations, authorizing and documenting changes that deviate from the baseline configuration and updating the baseline configuration as necessary, and verifying and documenting any changes from the baseline configuration.

The root cause of this violation was inadequate internal controls and training due to insufficient management oversight in the planning, preparation, and implementation of the change management requirements when transitioning to CIP Version 5.

SERC determined that this violation posed a serious risk to the reliability of the BPS. Attachment 13a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 13b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 13c provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2018019106

SERC determined that in 14 instances The Entities did not implement a documented process for several baseline configuration changes. These instances included a lack of documented process for (i) a change that deviates from the existing baseline configuration; (ii) determining required security controls in CIP-005 and CIP-007 before a change that could be impacted by the change; (iii) verifying that required security controls were not adversely affected after a change; and (iv) documenting the results of the verification.

The root cause of this violation was insufficient field procedures and inadequate associated functional testing, training, and oversight-related situational awareness.

SERC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Attachment 13d includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 13e include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 13e provides specific information on the Entities' Certification of Mitigation Plan Completion.

CIP-011-2 R1

SERC determined that The Entities were in noncompliance with CIP-011-2 R1 in three separate violations.

SERC2016016379

SERC determined that The Entities did not protect and securely handle BES Cyber System Information (BCSI) in accordance with their information protection system. The Entities stored a file containing BCSI on a corporate network shared drive, which The Entities did not identify in the information protection program as a BCSI repository.

The root cause of this violation was an oversight in procedures and training associated with the transition to CIP Version 5.

SERC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. Attachment 14a includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 14b include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 14b provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2016016572

SERC determined that in six instances The Entities did not protect and securely handle BCSI by failing to handle BCSI information in a controlled access repository in conformance with the documented information protection program.

The root cause of this violation was an oversight in procedures and training associated with the transition to CIP Version 5.

SERC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Attachment 14c includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted Mitigating Activities to address the referenced violation. Attachments 1 and 14d include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 14d provides specific information on the Entities' Certification of Mitigation Plan Completion.

SERC2017017564

SERC determined that in approximately [redacted] instances, The Entities' employees stored and transmitted shared account passwords to BCSs in a manner that did not conform to The Entities' documented information protection program. The Entities classified this information as BCSI in the information protection program.

The root cause of this violation was insufficient training.

SERC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Attachment 14e includes the facts regarding the violation that SERC considered in its risk assessment.

The Entities submitted their Mitigation Plan to address the referenced violation. Attachments 1 and 14f include a description of the mitigating activities The Entities took to address this violation.

The Entities certified that they had completed all mitigating activities. Attachment 14g provides specific information on the Entities' Certification of Mitigation Plan Completion.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of seven hundred and seventy-five thousand dollars ($775,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC considered the instant violations as repeat noncompliance with the CIP-006-6 R2 and CIP-007-3a R5, which served as an aggravating factor;
2. The Entities self-reported the violations;
3. The Entities were cooperative throughout the compliance enforcement process;
4. The Entities admitted to and accepted responsibility for the violations;
5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

6. The violations of SERC2017018774, SERC2016016492, SERC2017018548, SERC2016016339, and SERC2016016379 posed a minimal and not a serious or substantial risk to the reliability of the BPS;
7. The violations of SERC2016015954, SERC2017018136, SERC2017018279, SERC2017017286, SERC2017018440, SERC2017018441, SERC2017018467, SERC2017017236, SERC2017018246, SERC2018019200, SERC2018019106, SERC2016016572, and SERC2017017564 posed a moderate and not a serious or substantial risk to the reliability of the BPS;
8. The violations of SERC2016016548, SERC2017016832, and SERC2016016321 posed a serious and substantial risk to the reliability of the BPS; and
9. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of seven hundred and seventy-five thousand dollars ($775,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction, or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 18, 2019 and approved the resolution between SERC and The Entities. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the factors listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seven hundred and seventy-five thousand dollars ($775,000) is appropriate for the

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation,* "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation,* "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

For the reasons discussed below, NERC is requesting nonpublic treatment of certain portions of this filing pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. This filing contains sensitive information regarding the manner in which entities have implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publically, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC respectfully requests that the Commission designate the redacted portions of the Notice of Penalty as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113, respectively.[7]

a. <u>The Redacted Portions of this Filing Should Be Treated as Nonpublic Under Section 39.7(b)(4) as They Contain Information that Would Jeopardize the Security of the Bulk Power System if Publicly Disclosed</u>

Section 39.7(b)(4) of the Commission's regulations states:

The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise.

Consistent with its past practice, NERC is redacting information from this Notice of Penalty according to Section 39.7(b)(4) because it contains information that would jeopardize the security of the BPS if publicly disclosed. NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation.[8] Nonpublic treatment of redacted information, including the identity of the Entities and other details of the violations, depends on: 1) the nature of the CIP violations; 2) whether mitigation

[7] 18 C.F.R. § 388.113(e)(1).

[8] In response to recent Freedom of Information Act requests, the Commission has directed public disclosure regarding the disposition of CIP violations. *See, e.g.,* Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-19 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). In those cases, the Commission directed public disclosure of the identity of the registered entity; the Commission did not disclose other details regarding the CIP violations.

is complete; 3) the extent to which the disclosure of The Entities' identity would be useful to someone seeking to cause harm; 4) whether an audit has occurred since the violations; 5) whether the violations were administrative or technical in nature; and 6) the length of time that has elapsed since the filing of the Notice of Penalty.[9]

The redacted information in this Notice of Penalty includes details that could lead to identification of The Entities, and information about the security of The Entities' systems and operations, such as specific processes, configurations, or tools The Entities use to manage their cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of The Entities, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."[10]

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of The Entities and any information that could lead to their identification.[11] Information that could lead to the identification of The Entities includes The Entities' names, their NERC Compliance Registry ID, and information regarding the size and characteristics of The Entities' operations.

NERC is also treating as nonpublic any information about the security of The Entities' systems and operations.[12] Details about The Entities' systems, including specific configurations or the tools/programs they use to configure, secure, and manage changes to their BES Cyber Systems, would provide an adversary relevant information that could be used to perpetrate an attack on The Entities and similar entities that use the same systems, products, or vendors.

b. <u>The Redacted Portions of this Filing Should Also be Treated as CEII as the Information Could be Useful to a Person Planning an Attack on Critical Electric Infrastructure</u>

In addition to the provisions of Section 39.7(b)(4), the redacted information also separately qualifies for treatment as CEII under Section 388.113 of the Commission's regulations. CEII is defined, in relevant part, as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: (1) relates details about the production, generation, transmission, or distribution of energy; and (2) could be useful to a person planning an attack on critical infrastructure. As discussed above, this filing includes vulnerability and design information that could be

[9] FOIA No. FY19-30, Second Notice of Intent to Release (June 13, 2019).
[10] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204 at P 538 (*Order No. 672*).

[11] *See* the next section for a list of this information.
[12] *See* below for a list of this information.

useful to a person planning an attack on The Entities' critical infrastructure. The incapacity or destruction of The Entities' systems and assets would negatively affect national security, economic security, and public health and safety. For example, this Notice of Penalty includes the identification of specific cyber security issues and related vulnerabilities, as well as details concerning the types and configurations of The Entities' systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues.

In addition to the name of The Entities, the following information has been redacted from this Notice of Penalty:

1. BES Cyber System Information, including security procedures; information related to BES Cyber Assets; individual IP addresses with context; group of IP addresses; Electronic Security Perimeter diagrams that include BES Cyber Asset names, BES Cyber System names, IP addresses, IP address ranges; security information regarding BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, Electronic Access Control and Monitoring Systems that is not publicly available; and network topology diagrams, etc.
2. The names of The Entities' vendors and contractors.
3. The NERC Compliance Registry numbers of The Entities.
4. The registered functions and registration dates of The Entities.
5. The names of The Entities' facilities.
6. The names of The Entities' assets.
7. The names of The Entities' employees.
8. The names of departments that are unique to The Entities.
9. The sizes and scopes of The Entities' operations.

Under Section 388.113, NERC requests that the CEII designation apply to the redacted information in Items 1-2 for five years from this filing date, June 27, 2019. Details about The Entities' operations, networks, and security should be treated and evaluated separately from their identity to avoid unnecessary disclosure of CEII that could pose a risk to security. NERC requests that the CEII designation apply to the redacted information from Items 3-9 for three years from this filing date, June 27, 2019. NERC requests the CEII designation for three years to allow for several activities that should reduce the risk to the security of the BPS. Those activities include, among others:

1. Compliance monitoring of The Entities to ensure sustainability of the improvements described in this Notice of Penalty; and
2. Remediation of any subsequent violations discovered through compliance monitoring by SERC.

The Entities should be less vulnerable to attempted attacks following these activities. After three years, disclosure of the identity of The Entities may pose a lesser risk than it would today.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

1. Settlement Agreement by and between SERC and the Entities executed April 17, 2019, included as Attachment 1;
2. Record documents for the violation of CIP-002-5.1 R1 included as Attachment 2;
    a. The Entities' Self-Report (SERC2016015954)
    b. The Entities' Mitigation Plan designated as SERCMIT014422 submitted February 8, 2019.
    c. The Entities' Certification of Mitigation Plan Completion submitted April 19, 2019.
3. Record documents for the violations of CIP-004-6 R5 included as Attachment 3;
    a. The Entities' Self-Report (SERC2017018136)
    b. The Entities' Certification of Mitigation Plan Completion submitted September 15, 2017
    c. The Entities' Self-Report (SERC2017018279)
    d. The Entities' Certification of Mitigation Plan Completion submitted September 22, 2017
4. Record documents for the violation of CIP-005-5 R1 included as Attachment 4;
    a. The Entities' Self-Report (SERC2017018774)
    b. The Entities' Certification of Mitigation Plan Completion submitted December 18, 2017
5. Record documents for the violation of CIP-005-5 R2 included as Attachment 5;
    a. The Entities' Self-Report (SERC2016016548)
    b. The Entities' Mitigation Plan designated as SERCMIT014395 submitted August 17, 2018
    c. The Entities' Certification of Mitigation Plan Completion submitted August 17, 2018
6. Record documents for the violation of CIP-006-6 R1 included as Attachment 6;
    a. The Entities' Self-Report (SERC2017017286)
    b. The Entities' Mitigation Plan designated as SERCMIT014400 submitted June 26, 2018
    c. The Entities' Certification of Mitigation Plan Completion submitted June 26, 2018
7. Record documents for the violations of CIP-006-6 R2 included as Attachment 7;
    a. The Entities' Self-Report (SERC2017018440)
    b. The Entities' Certification of Mitigation Plan Completion submitted January 23, 2018
    c. The Entities' Self-Report (SERC2017018441)
    d. The Entities' Certification of Mitigation Plan Completion submitted April 18, 2019
8. Record documents for the violation of CIP-007-6 R1 included as Attachment 8;
    a. The Entities' Self-Report (SERC2016016492)
    b. The Entities' Certification of Mitigation Plan Completion submitted January 19, 2017
9. Record documents for the violation of CIP-007-6 R2 included as Attachment 9;
    a. The Entities' Self-Report (SERC2017018467)
    b. The Entities' Certification of Mitigation Plan Completion submitted October 11, 2017
10. Record documents for the violation of CIP-007-6 R3 included as Attachment 10;

a. The Entities' Self-Report (SERC2017017236)
b. The Entities' Mitigation Plan designated as SERCMIT014396 submitted July 10, 2018
c. The Entities' Certification of Mitigation Plan Completion submitted July 10, 2018

11. Record documents for the violation of CIP-007-3a R5 included as Attachment 11;
    a. The Entities' Self-Report (SERC2017016832)
    b. The Entities' Mitigation Plan designated as SERCMIT014423 submitted February 8, 2019
    c. The Entities' Certification of Mitigation Plan Completion submitted February 8, 2019
12. Record documents for the violations of CIP-007-6 R5 included as Attachment 12;
    a. The Entities' Self-Report (SERC2017018246)
    b. The Entities' Mitigation Plan designated as SERCMIT014398 submitted July 12, 2018
    c. The Entities' Certification of Mitigation Plan Completion submitted July 12, 2018
    d. The Entities' Self-Report (SERC2018019200)
    e. The Entities' Mitigation Plan designated as SERCMIT014399 submitted July 23, 2018
    f. The Entities' Certification of Mitigation Plan Completion submitted July 23, 2018
    g. The Entities' Self-Report (SERC2017018548)
    h. The Entities' Certification of Mitigation Plan Completion submitted December 6, 2017
    i. The Entities' Self-Report (SERC2016016339)
    j. The Entities' Certification of Mitigation Plan Completion submitted October 26, 2016
13. Record documents for the violations of CIP-010-2 R1 included as Attachment 13;
    a. The Entities' Self-Report (SERC2016016321)
    b. The Entities' Mitigation Plan designated as SERCMIT014426 submitted February 8, 2019
    c. The Entities' Certification of Mitigation Plan Completion submitted February 8, 2019
    d. The Entities' Self-Report (SERC2018019106)
    e. The Entities' Certification of Mitigation Plan Completion submitted April 27, 2018
14. Record documents for the violations of CIP-011-2 R1 included as Attachment 14;
    a. The Entities' Self-Report (SERC2016016379)
    b. The Entities' Certification of Mitigation Plan Completion submitted December 8, 2016
    c. The Entities' Self-Report (SERC2016016572)
    d. The Entities' Certification of Mitigation Plan Completion submitted March 1, 2019
    e. The Entities' Self-Report (SERC2017017564)
    f. The Entities' Mitigation Plan designated as SERCMIT014401 submitted September 4, 2018
    g. The Entities' Certification of Mitigation Plan Completion submitted September 4, 2018

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. Jason Blake President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8204 (704) 357-7914 – facsimile jblake@serc1.org Holly A. Hawkins* General Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 hhawkins@serc1.org Jimmy C. Cline* Managing Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 414-5259 jccline@serc1.org Rebecca A. Poulsen* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 414-5230 rpoulsen@serc1.org	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Jill Goatcher* Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile jill.goatcher@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Jill Goatcher

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Jill Goatcher
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net
jill.goatcher@nerc.net

cc: The Entities
SERC Reliability Corporation

Attachment 1

Settlement Agreement by and between SERC and the

Entities executed April 17, 2019

[redacted]

CUI//CEII – DO NOT RELEASE
Document Contains Critical Energy/Electric Infrastructure Information (CEII)

SETTLEMENT AGREEMENT

AMONG SERC RELIABILITY CORPORATION

AND

[redacted]

I. INTRODUCTION

1. SERC Reliability Corporation (SERC) and [redacted] enter into this Settlement Agreement (Settlement Agreement) to resolve Alleged Violations by the [redacted] of the below-referenced Reliability Standards and Requirements.[1] SERC and the [redacted] are each referred to as a "Party" and collectively as "Parties."

Reliability Standard	Requirement	SERC Tracking No.	NERC Tracking No.	Entity
CIP-002-5.1	R1, Part 1.2	SERC2016-402419	SERC2016015954	[redacted]
CIP-004-6	R5, Part 5.1	SERC2017-402808	SERC2017018136	[redacted]
CIP-004-6	R5, Part 5.2	SERC2017-402830	SERC2017018279	[redacted]
CIP-005-5	R1, Part 1.1	SERC2017-402923	SERC2017018774	[redacted]
CIP-005-5	R2, Part 2.1	SERC2016-402543	SERC2016016548	[redacted]
CIP-006-6	R1, Part 1.2	SERC2017-402649	SERC2017017286	[redacted]
CIP-006-6	R2, Part 2.1 & 2.2	SERC2017-402867	SERC2017018440	[redacted]
CIP-006-6	R2, Part 2.1 & 2.2	SERC2017-402868	SERC2017018441	[redacted]
CIP-007-6	R1, Part 1.1	SERC2016-402526	SERC2016016492	[redacted]
CIP-007-6	R2, Part 2.3	SERC2017-402870	SERC2017018467	[redacted]
CIP-007-6	R3, Part 3.1	SERC2017-402643	SERC2017017236	[redacted]
CIP-007-3a	R5, R.5.2.1 & 5.3.3	SERC2017-402615	SERC2017016832	[redacted]
CIP-007-6	R5, Part 5.1	SERC2017-402822	SERC2017018246	[redacted]

[1] This Agreement references the version of the Reliability Standard in effect at the time each Alleged Violation began. [redacted] however, committed to perform mitigating actions to comply with the most recent version of each Reliability Standard Requirement.

[redacted]

CIP-007-6	R5, Part 5.2 & 5.4	SERC2018-402985	SERC2018019200 [redacted]
CIP-007-6	R5, Part 5.4	SERC2017-402876	SERC2017018548 [redacted]
CIP-007-6	R5, Part 5.5.1	SERC2016-402499	SERC2016016339 [redacted]
CIP-010-2	R1, Part 1.1, 1.2, 1.3, & 1.4	SERC2016-402496	SERC2016016321 [redacted]
CIP-010-2	R1, Part 1.4	SERC2018-402974	SERC2018019106 [redacted]
CIP-011-2	R1, Part 1.2	SERC2016-402511	SERC2016016379 [redacted]
CIP-011-2	R1, Part 1.2	SERC2016-402548	SERC2016016572 [redacted]
CIP-011-2	R1, Part 1.2	SERC2017-402689	SERC2017017564 [redacted]

2. The Parties stipulate to the facts in this Agreement for the sole purpose of resolving the Alleged Violations. The [redacted] admit that these facts constitute Alleged Violations of the above-referenced Reliability Standard Requirements.

II. OVERVIEW OF [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

III. EXECUTIVE SUMMARY

6. This settlement resolves 21 self-reported Alleged Violations of the CIP Reliability Standards. These Alleged Violations include violations of CIP versions 3 and 5 self-reported from 2016 through early 2018. Of the 21 violations, SERC determined that three (3) violations posed a serious and substantial risk to the reliability of the Bulk Power System (BPS), 13 violations posed a moderate risk to the BPS, and the remaining five (5) violations posed a minimal risk to the reliability of the BPS.

7. A contributing cause to the Alleged Violations was organizational silos between management and those responsible across multiple business units for implementing the compliance procedures. Following the major expansion of scope and implementation of CIP version 5, effective July 1, 2016, some [redacted] business units were still very new to CIP compliance, and many of the new employees within these business units underwent a steep learning curve. In the early stages of CIP version 5 in 2016 and 2017, [redacted] was still in the process of formalizing its CIP Internal Controls Program (ICP) and the detective controls contained therein.

8. For most of the Alleged Violations, [redacted] documented procedures, which if implemented, correctly would avoid noncompliance. However, in practice, internal controls were lacking to ensure adherence to the procedures, which created inconsistent application of the procedures. Additionally, in some cases, training on procedures was lacking, which was compounded by business units and employees being new to CIP compliance, which created confusion as to expectations and ownership of specific activities. Nonetheless, [redacted] discovered the noncompliance and timely submitted self-reports and mitigation activities to SERC, which demonstrates [redacted] strong culture and commitment to security and compliance, and employee awareness and adherence to the tenants of its Internal Compliance Program.

9. To address the overarching failure to fully implement procedures due to lack of internal controls and inadequate training, through the 2016-2018 development of the formalized CIP ICP and documented mitigations of existing issues, several improvements were made to business unit-specific processes and oversight to improve preventative and detective controls over the course of 2017 and 2018. Many lessons learned from the earlier implementation of the O&P ICP were carried over into the formalization and implementation of the CIP ICP. In addition, in 2018, [redacted] received funding approval to add more dedicated resources to an overall ICP department [redacted] to cover both O&P and CIP internal controls. Specific to CIP internal compliance, the new department implemented [redacted] in Q3 and Q4 of 2018 that includes [redacted] CIP controls, which will be expanded to [redacted] CIP controls later in 2019 based on the revised 2019 Reliability Standards Risk Assessment.

IV. ADJUSTMENT FACTORS

10. In addition to the facts and circumstances stated above, SERC considered the following factors in its sanction determination:

Self-Identification and Self-Reporting

11. The [redacted] self-identified and reported all of the Alleged Violations at issue in this Agreement. In 2016, [redacted] implemented a formal internal controls program, called the [redacted] The [redacted] program identifies and documents [redacted] strong internal controls across its business units and functions. The [redacted] program includes performing and documenting independent testing of key controls, developing action plans to address any deficiencies identified during testing, and tracking completion of those action plans. SERC seeks to encourage [redacted], which led to timely self-reporting by awarding mitigation credit.

Cooperation

12. SERC considered the [redacted] cooperation during the compliance monitoring and enforcement processes and awarded mitigating credit. The [redacted] were cooperative during the Compliance Audit and throughout the enforcement processes and were forthcoming with detailed information to SERC. The [redacted] have been open with SERC regarding Alleged Violations, systems, and organization, allowing SERC to better analyze the Alleged Violations.

Compliance History

13. When assessing the penalty for the Alleged Violations at issue in this Agreement, SERC considered whether the facts of these Alleged Violations constitute repetitive infractions. The [redacted] have prior violations of similar conduct to the current Alleged Violations of CIP-006-6 R2; P2.1[2] and CIP-007-3a R5.[3] Therefore, SERC considered the repeat conduct as an aggravating factor for penalty purposes.

---

[2] CIP-006-6 R2, P2.1 requires visitors with unauthorized physical access to be continuously monitored within PSPs. The former standard covering the continuous escort of visitors within PSPs is CIP-006-3c R1. [redacted] prior violations of CIP-006-3c R1 (SERC2013011699, SERC2013011706, and SERC2013012710), which constitute repeat conduct of the current Alleged Violation CIP-006-6 R2; P2.1, were included in the same settlement agreement [redacted] and was filed with FERC on [redacted] and approved by FERC on [redacted]

[3] CIP-007-3a R5 requires in part the changing password for system accounts. [redacted] prior violations (SERC201000618—CIP-007-1 R5.3.3) and SERC201000614—CIP-006-1 R1.8), which constitute repeat conduct with the current Alleged Violations of CIP-007-3a R5 were filed in the same settlement agreement [redacted] and was filed with FERC on [redacted] and approved by FERC on [redacted]

V. PENALTY OR SANCTION

14. Based upon the foregoing, the [redacted] shall pay a monetary penalty of $775,000 in total to SERC.

15. The [redacted] shall remit the payment to SERC via check or by wire transfer to an account to be identified by SERC within 30 days after the Agreement is either approved by the (Commission) or by operation of law. SERC shall notify NERC, and NERC shall notify the Commission, if the payment is not timely received. If the [redacted] do not remit the payment by the required date, interest payable to SERC will begin to accrue pursuant to the Commission's regulations at 18 C.F.R. §35.19a(a)(2)(iii) from the date that payment is due, and shall be payable in addition to the payment.

16. Failure to make a timely penalty payment or to comply with any of the terms and conditions agreed to herein, or any other conditions of this Settlement Agreement shall be deemed to be either the same alleged violations that initiated this Settlement Agreement and/or additional violations and may subject the [redacted] to new or additional enforcement, penalty or sanction actions in accordance with the NERC Rules of Procedure. The [redacted] shall retain all rights to defend against such additional enforcement actions in accordance with NERC Rules of Procedure.

VI. ADDITIONAL TERMS

17. The Parties agree that this Agreement is in the best interest of Bulk Electric System (BES) reliability. The terms and conditions of the Agreement are consistent with the regulations and orders of the Commission and the NERC Rules of Procedure.

18. SERC shall report the terms of all settlements of compliance matters to NERC. NERC will review the Agreement for the purpose of evaluating its consistency with other settlements entered into for similar violations or under similar circumstances. Based on this review, NERC will either approve or reject this Agreement. If NERC rejects the Agreement, NERC will provide specific written reasons for such rejection and SERC will attempt to negotiate with the [redacted] a revised settlement agreement that addresses NERC's concerns. If a settlement cannot be reached, the enforcement process will continue to conclusion. If NERC approves the Agreement, NERC will (a) report the approved settlement to the Commission for review and approval by order or operation of law and (b) publicly post the Alleged Violation and the terms provided for in this Agreement.

19. This Agreement binds the Parties upon execution, and may only be altered or amended by written agreement executed by the Parties. The [redacted] expressly waives its right to any hearing or appeal concerning any matter set forth herein, unless and only to the extent that the [redacted] contend that

[redacted]

any NERC or Commission action constitutes a material modification to this Agreement.

20. SERC reserves all rights to initiate enforcement action against the [redacted] in accordance with the NERC Rules of Procedure in the event that the [redacted] fails to comply with any of the terms or conditions of this Agreement. The [redacted] retain all rights to defend against such action in accordance with the NERC Rules of Procedure.

21. The [redacted] consent to SERC's future use of this Agreement for the purpose of assessing the factors within the NERC Sanction Guidelines and applicable Commission orders and policy statements, including, but not limited to, the factor evaluating the [redacted] violation history. Such use may be in any enforcement action or compliance proceeding undertaken by NERC or any Regional Entity or both, provided however that the [redacted] do not consent to the use of the conclusions, determinations, and findings set forth in this Agreement as the sole basis for any other action or proceeding brought by NERC or any Regional Entity or both, nor do the [redacted] consent to the use of this Agreement by any other party in any other action or proceeding.

22. The [redacted] affirm that all of the matters set forth in this Agreement are true and correct to the best of its knowledge, information, and belief, and that it understands that SERC enters into this Agreement in express reliance on the representations contained herein, as well as any other representations or information provided by the [redacted] to SERC during any [redacted] interaction with SERC relating to the subject matter of this Agreement.

23. Upon execution of this Agreement, the Parties stipulate that the Possible Violation addressed herein constitutes an Alleged Violation. The Parties further stipulate that all required, applicable information listed in Section 5.3 of the CMEP is included within this Agreement.

24. Each of the undersigned agreeing to and accepting this Agreement warrants that he or she is an authorized representative of the party designated below, is authorized to bind such party, and accepts the Agreement on the party's behalf.

25. The undersigned agreeing to and accepting this Agreement warrant that they enter into this Agreement voluntarily and that, other than the recitations set forth herein, no tender, offer, or promise of any kind by any member, employee, officer, director, agent, or representative of the Parties has been made to induce the signatories or any other party to enter into this Agreement.

26. The Agreement may be signed in counterparts.

27. This Agreement is executed in duplicate, each of which so executed shall be deemed to be an original.

[redacted]

SIGNATURE PAGE TO FOLLOW[4]

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

[4] An electronic version of this executed document shall have the same force and effect as the original.

[redacted]

[redacted]

[redacted]

Agreed to and accepted by:

SERC RELIABILTIY CORPORATION

Jason Blake
President and Chief Executive Officer

4-17-19
Date

Attachment A

I. ALLEGED VIOLATIONS

A. CIP-002-5.1 R1, Part 1.2 (SERC2016015954)

1. CIP-002-5.1 ensures the identification and categorization of BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

2. CIP-002-5.1 R1 states in relevant part:

> **R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:
>
> i. Control Centers and backup Control Centers;
> ii. Transmission stations and substations;
> iii. Generation resources;
> iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
> v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
> vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.
>
> **1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;
> **1.2.** Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and
> **1.3.** Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Description of Alleged Violation and Risk Assessment for SERC2016015954

3. On [redacted] SERC sent [redacted] an audit detail letter (ADL) notifying it of a Compliance Audit scheduled for [redacted] through [redacted] with the on-site week being the week of [redacted]

4. On [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in violation of CIP-002-5.1 R1, Part 1.2. *See* Self-Report for

Attachment A

SERC2016015954. [redacted] failed to properly classify [redacted] medium impact BES Cyber Systems (BCSs) by the CIP Version 5 effective date of July 1, 2016.

5. During November of 2015, [redacted] discovered that it had not identified [redacted] servers, located at [redacted] data centers, as [redacted] medium impact BCSs ([redacted] also classified these as [redacted] BES Cyber Assets (BCAs)). [redacted] had identified these servers as low impact BCS because they monitored and operated low impact BCS and associated transmission Facilities at [redacted] transmission substations. However, since the control communications originated from the [redacted] control centers and energy management system (EMS), and went out to these substations via the Distributed Supervisor Control and Data Acquisition (DSCADA) system at the substations, [redacted] should have identified these [redacted] DSCADA devices as medium impact BCS. [redacted]

6. On January 5, 2016, [redacted] and [redacted] representatives met with SERC to discuss the situation, and [redacted] explained how it would address the situation going forward. Specifically, [redacted] developed a prioritized risk-based conversion plan of the substations communications to transition control from DSCADA to EMS.

7. [redacted] executed the conversion plan and limited the use of the [redacted] servers to control only [redacted] low impact substations by eliminating their use of DSCADA commands and routing communications directly from the high impact EMS to the low impact substation devices.

8. [redacted] conducted an extent-of-condition assessment across the [redacted] footprint looking for and examining communications configurations that employed the same legacy technology at issue here. [redacted] did not find any further instances of noncompliance.

9. The root cause of this violation was management oversight in planning and implementing the transition to CIP Version 5.

10. This violation began on July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended on September 7, 2017, when [redacted] finished eliminating the use of DSCADA for the [redacted] involved devices.

11. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[3] By not identifying medium impact BCSs, there is a possible risk in not affording defense-in-depth protections to those BCSs in accordance with CIP Version 5, increasing the risk that malicious actors could access, modify, operate or hinder grid operations and compromise security. However, in this case, the BCSs operable at substations via the unidentified BCSs were all low impact. The legacy controls employed by [redacted] afforded reasonable security including physical and electronic protections. [redacted] physically secured the

[3] According to the CIP-002-5.1 Table of Compliance Elements, this noncompliance warrants a "High" VRF and a "Lower" VSL.

BCSs with biometric and card readers. Electronic protections included no direct internet or corporate network access to the BCSs by using separate virtual private networks protected behind firewalls. Further, device and network monitoring and system logging was in place at all times, with antivirus and malware prevention installed.

Mitigating Actions for SERC2016015954

12. On February 8, 2019, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-002-5.1 R1, Part 1.2. *See* Mitigation Plan for SERC2016015954. On March 5, 2019, SERC accepted the Mitigation Plan.

13. To mitigate this violation, [redacted]

    i. developed a conversion plan that removed the DSCADA controls from all [redacted] substations containing Low Impact BES Cyber Systems by implementing additional communication paths, and adjusted the RTUs and EMS databases to poll the transmission devices directly from the EMS; and

    ii. completed the conversion plan ahead of schedule.

14. On April 19, 2019, [redacted] certified to SERC that it completed the Mitigation Plan on September 7, 2017. *See* Certification of Mitigation Plan Completion for SERC2016015954.

B. CIP-004-6 R5 (SERC2017018136 and SERC2017018279)

14. CIP-004-6 reduces the risk of compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

15. CIP-004-6 R5 states in relevant part:

    R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

    P5.1. A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).

    P5.2. For reassignments or transfers, 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.

Description of Alleged Violation and Risk Assessment for SERC2017018136

16. On August 7, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-004-6 R5. *See* Self-Report for SERC2017018136. SERC later determined [redacted] was specifically in violation of CIP-004-6 R5, Part 5.1. In two instances, [redacted] did not initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action.

17. On May 1, 2017, an employee retired from [redacted] Prior to the effective retirement date, [redacted] had removed all of the retiree's CIP-related access with the exception of remote access to the corporate network, which facilitated and provisioned access to two repositories housing transmission substations-related BES Cyber System Information (BCSI). The first BCSI repository housed engineering design information, firewall requests, network topologies, and working research information on CIP Cyber Assets. The second BCSI repository housed BES Cyber System asset and BES Facility lists, vulnerability assessments, and port scans for substation and IT networks.

18. On May 5, 2017, during the off-boarding process, the retiree's former manager realized an oversight had occurred in not removing the retiree's ability for remote access to the corporate network and access to BCSI and contacted HR to resolve. On May 8, 2017, [redacted] removed the retiree's remote access to the corporate network and access to BCSI by disabling the corporate network ID.

19. On June 1, 2017, another employee retired from [redacted] At the time of termination, [redacted] did not collect the individual's physical ID badge, and as a result, the retiree retained the ability for unescorted physical access to one CIP Physical Security Perimeter (PSP) server cabinet containing Electronic Access Control or Monitoring System (EACMSs) associated with transmission substations Medium Impact BCSs, and a Physical Access Control Systems (PACSs) server associated with all High and Medium Impact PSPs. In addition, [redacted] did not disable the retiree's network ID upon termination, which facilitated remote access to the corporate network and the ability to access an energy management system (EMS) BCSI repository and access to [redacted] EACMS Cyber Assets.

20. On June 9, 2017, the retiree's former manager realized the oversight in access removals and submitted the required employment status change paperwork to HR.

Later that day, [redacted] disabled the retiree's corporate network ID, resulting in the removal of remote access to the corporate network and all aforementioned electronic access. On June 10, 2017, [redacted] removed the retiree's PSP access by disabling the ID badge in the PACS system.

21. On June 23, 2017, [redacted] conducted an extent-of-condition assessment by performing an internal control review of Q2 2017 employee terminations and associated CIP access removals and revocations. [redacted] did not find any further instances of noncompliance.

22. The root cause of this violation was training deficiencies in access revocation procedures.

23. This violation started May 2, 2017, when [redacted] should have revoked the first retiree's remote access to the corporate network, and ended on June 10, 2017, when [redacted] revoked the second retiree's PSP access.

24. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[4] [redacted] failure to revoke remote access to the corporate network and unescorted physical access to PSPs as required enhanced the risk that a bad actor could access sensitive information about the EMS system or EACMSs and PACSs and potentially gain access to BCSs. However, the collective duration of the two instances was only 13 days. Each of the two retirees had a minimum of 30 years of company service, were in good standing with [redacted] and had up-to-date personnel risk assessments and cyber security training. [redacted] confirmed that the former employees did not attempt to access BCSs.

Mitigating Actions for SERC2017018136

25. On August 7, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-004-6 R5, Part 5.1. *See* Mitigation Plan for SERC2017018136. On February 18, 2019, SERC accepted the Mitigation Plan.

26. To mitigate this violation, [redacted]

    i. conducted a review of all terminated [redacted] employees and contractors with CIP access;

    ii. physical security operations team reviewed PACS logs to determine if the [redacted] employee attempted to physically access any CIP areas after June 1, 2017;

[4] According to the CIP-004-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "High" VSL.

iii. conducted a retraining with managers within the applicable business units on the access management revocation program and their responsibilities as a manager; and

iv. disseminated a reinforcement message to reiterate manager's responsibilities for revoking CIP access on or before the effective date of termination.

27. On September 15, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of September 15, 2017. *See* Certification of Mitigation Plan Completion for SERC2017018136.

Description of Alleged Violation and Risk Assessment for SERC2017018279

28. On August 29, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-004-6 R5, Part 5.2. *See* Self-Report for SERC2017018279. For a reassignment, [redacted] did not revoke an individual's authorized electronic access to individual accounts by the end of the next calendar day following the date that [redacted] determined that the individual no longer required retention of that access.

29. On April 5, 2016, a [redacted] employee transferred to a new position within the company. At the time, management determined that the employee had a business need to retain certain electronic access until November 4, 2016.

30. On November 4, 2016, [redacted] revoked the employee's electronic access in the access management application and also revoked electronic access to the primary EMS servers. However, [redacted] did not revoke electronic access to the backup EMS system because the analyst responsible for revoking access had mistyped the username of the transferred employee and when the username was not found, the analyst erroneously assumed that [redacted] previously removed the access. As a result, the employee retained access to one data center, including one High Impact BCS and [redacted] BCAs.

31. On June 29, 2017, while performing a comparison of domain access on the primary EMS system versus the backup EMS system, [redacted] noted this discrepancy in the transferred employee's domain access where there should have been none. [redacted] considered this comparison the extent of condition assessment and found no other similar discrepancies. The same day, [redacted] revoked access to the backup EMS system, fully completing revocation of the transferred employee's access.

32. [redacted] did not find this discrepancy during its quarterly access reviews because the individual performing those reviews thought revoking the username in the primary system would automatically revoke access in the backup system because that was how [redacted] configured other similar systems. However, [redacted]

configured the system involved differently and it required revocation separately on each the primary and backup.

33. The root cause of this noncompliance was lack of detailed procedures regarding removing access and lack of emphasis on training regarding the quarterly reviews.

34. This violation started on November 6, 2016, when [redacted] should have revoked electronic access, and ended June 29, 2017, when [redacted] revoked access.

35. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[5] [redacted] failure to revoke electronic access to the backup EMS when it was no longer needed could have allowed malicious actors to gain control of it and make harmful configuration or other changes affecting grid security. However, the backup EMS system employed defense-in-depth provisions against cyber-attack. The backup EMS system was only in use for two days during the violation time-period. [redacted] also had situational awareness tools in service, including active monitoring comparisons of primary and backup system configurations and specifically the capability to discover and report attempts to change the configuration of the backup EMS.

Mitigating Actions for SERC2017018279

36. On August 29, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-004-6 R5, Part 5.2. *See* Mitigation for SERC2017018279. On February 18, 2019, SERC accepted the Mitigation Plan.

37. To mitigate this violation, [redacted]

    i. EMS compliance conducted a meeting to assess the scope and the root cause of the issue;
    ii. to determine the extent of condition, EMS compliance conducted a review of access between the [redacted] node ([redacted] and EMS [redacted] system ([redacted] systems to determine any other existing discrepancies;
    iii. EMS compliance conducted training with appropriate staff on provisioning and revocation applicable to [redacted] and [redacted] assets to ensure both stay in sync going forward; and
    iv. EMS compliance worked with operations to develop a monthly assurance review comparing the [redacted] to [redacted] to ensure they remain in sync.

[5] According to the CIP-004-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Moderate" VSL.

38. On September 22, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of September 22, 2017. *See* Certification of Mitigation Plan Completion for SERC2017018279.

C. CIP-005-5 R1, Part 1.1 (SERC2017018774)

39. CIP-005-5 ensures the management of electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP) in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

40. CIP-005-5 R1 states in relevant part:

> **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.
>
> **P1.1.** All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.

Description of Alleged Violation and Risk Assessment for SERC2017018774

41. On December 12, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in noncompliance with CIP-005-5 R1, Part 1.1. *See* Self-Report for SERC2017018774. [redacted] had one instance where it failed to ensure an applicable Cyber Asset was connected to a network via a routable protocol resided within a defined ESP.

42. On September 12, 2017, a field support employee connected an applicable Cyber Asset, a Remote Terminal Unit (RTU), to a network device located outside a substation ESP. Specifically, while the employee performed an authorized network configuration change to remove a device from the ESP, the employee mistakenly disconnected the wrong device, an RTU, from the ESP firewall and connected it to a network router via a routable protocol outside the ESP. The RTU was classified as a BES Cyber Asset (BCA) and a BES Cyber System (BCS) and resided inside a medium impact substation.

43. On September 13, 2017, a [redacted] employee discovered the issue when the employee could not access the RTU during post-field work network testing.

44. On September 14, 2017, [redacted] dispatched an employee to determine the cause of the issue. The [redacted] employee discovered the errant configuration and corrected it the same day.

45. [redacted] performed an extent-of-condition assessment by reviewing all similar substation network configuration changes across [redacted] and confirmed that it successfully implemented all similar network configuration changes.

46. The root causes of this violation were insufficiently granular fieldwork procedures for removing devices from within ESPs and inadequate training for carrying out these activities.

47. This violation started September 12, 2017, when [redacted] connected the RTU outside the ESP, and ended on September 14, 2017, when [redacted] reconnected the RTU inside the ESP.

48. This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS.[6] By not ensuring that applicable Cyber Assets connected via routable protocol resided within an ESP, there was a potential for parties to gain control of the RTU and associated BES Facilities and cause grid instability. However, the RTU remained inside a PSP and hardened against malicious code, with security patches up-to-date. [redacted] configured the RTU to be isolated from the internet and configured the connected network router outside the ESP such that the static Internet Protocol address of the RTU was not accessible to a wide area. The connection was for engineering access only and no one used the connection in the timeframe to know it was unavailable. [redacted] experienced no data issues due to this noncompliance and no data traversed this connection to populate EMS or affect anything operationally. The RTU had a different connection that provided data to the EMS, which was unaffected.

Mitigating Actions for SERC2017018774

49. On December 12, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-005-5 R1, Part 1.1. *See* Mitigation Plan for SERC2017018774. On February 18, 2019, SERC accepted the Mitigation Plan.

50. To mitigate this violation, [redacted]

    i. removed the RTU from the external substation network and reconnected the device to the CIP ESP firewall. [redacted] also provided evidence demonstrating the RTU was patched properly while it was outside the ESP;
    ii. performed an issue investigation and human performance learning event to determine and document the root cause of the issue;
    iii. updated the substation work practice based on the results of the investigation to clarify the configuration change process and add steps in the process to prevent future recurrence;
    iv. performed retraining with field services personnel on the changes to the substations work practice to reinforce new process steps intended to prevent future recurrence;

[6] According to the CIP-005-5 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

v. performed a network analysis documenting the ESP and substation wide area network configuration; and

vi. to determine the extent of condition, reviewed all completed substation changes related to the implementation and confirm all BCAs are accounted for and properly secured behind ESP firewalls.

51. On December 18, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of December 18, 2017. *See* Certification of Mitigation Plan Completion for SERC2017018774 for SERC2017018774.

D. CIP-005-5 R2, Part 2.1 (SERC2016016548)

52. CIP-005-5 requires the management of electronic access to BES Cyber Systems by specifying a controlled ESP in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

53. CIP-005-5 R2 states in relevant part:

> **R2.** Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.
>
> **R2.1** Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

Description of Alleged Violation and Risk Assessment for SERC2016016548

54. On November 18, 2016, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in violation of CIP-005-5 R2, Part 2.1. *See* Self-Report for SERC2016016548. [redacted] allowed Interactive Remote Access (IRA) to BES Cyber Systems (BCSs) without using an Intermediate System.

55. [redacted] failed to implement adequate technical controls on or before July 1, 2016 to prevent remote access from bypassing the IRA Intermediate System (IRA-IS). On July 15, 2016, an EMS employee discovered and reported an ability to bypass the IRA-IS from outside an ESP using an individual user account on an energy management system (EMS) testing-related Cyber Asset and connecting via a specific port to access BES Cyber Assets (BCAs) residing within an Electronic Security Perimeter (ESP). An individual who bypassed the IRA-IS could have accessed the entire EMS system from outside the ESP.

56. On August 12, 2016, [redacted] completed an extent-of-condition assessment by reviewing EMS network traffic logs from July 1, 2016, when Version 5 of the Standard and Requirement became mandatory and enforceable, through August 11, 2016, the day before [redacted] started the extent-of-condition assessment. The

specific port involved in the access is only used on control centers and the EMS. [redacted] identified and assessed similar instances where users bypassed the IRA-IS using a similar means. [redacted] found [redacted] other employees who had also bypassed the IRA-IS using a shared account.

57. The root cause of this violation was determined to be oversights in the documented procedures related to utilizing the IRA-IS. Specifically, [redacted] failed to guard against using the port to bypass the IRA-IS because it implemented the port for a specific other purpose.

58. This violation started July 1, 2016, when the Standard and Requirement became mandatory and enforceable under CIP Version 5, and ended August 10, 2016, when a [redacted] employee last used this unauthorized access method.

59. This violation posed a serious risk to the reliability of the BPS.[7] By not utilizing IRA-IS to access applicable Cyber Assets from outside ESPs, there is a potential for remote users to gain operational control of cyber assets and BPS facilities and maliciously cause grid instability. However, the [redacted] employees had authorized access privileges to all applicable Cyber Assets within the ESP. The [redacted] employees had current personnel risk assessments and cyber security training. All traffic initiated from Cyber Assets outside the ESP was encrypted and required multi-factor authentication between that Cyber Asset and any BCA.

Mitigating Actions for SERC2016016548

60. On August 17, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-005-5 R2, Part 2.1. *See* Mitigation Plan for SERC2016016548. On February 18, 2019, SERC accepted the Mitigation Plan.

61. To mitigate this violation [redacted]

i. reviewed EMS network traffic logs and conducted staff interviews to determine if any additional users bypassed the IRA solution using similar means;
ii. conducted training and provided instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP;
iii. conducted another training/counseling session with EMS staff on the unauthorized usage of secured communications protocol over the involved port;
iv. completed the implementation of restricting the involved port at [redacted] EMS ESPs, where possible;
v. completed the implementation of restricting the involved port usage at the remaining [redacted] EMS ESPs, where possible; and

[7] According to the CIP-005-5 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Moderate" VSL.

vi. completed updates to the involved EMS system to restrict user/system access, and will log, monitor, and alert on unapproved secured communications protocol usage.

62. On August 17, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of June 26, 2017. *See* Certification of Mitigation Plan Completion for SERC2016016548.

E. CIP-006-6 R1 (SERC2017017286)

63. CIP-006-6 requires the management of physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

64. CIP-006-6 R1 states in relevant part:

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.

P1.2. 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.

. . . .

P1.10. Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- encryption of data that transits such cabling and components; or
- monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- an equally effective logical protection.

65. On March 24, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-006-6 R1, Part 1.2. *See* Self-Report for [redacted] had one instance where it did not use at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter (PSP) to only those individuals who have authorized unescorted physical access.

66. On December 5, 2016, a [redacted] employee reported a lost badge. [redacted] replaced the lost badge with a new one, and updated the non-CIP badging system to reflect the change to the new badge. However, [redacted] did not also update the CIP Physical Access Control System (PACS) employee badge system and the lost badge continued to permit access into [redacted] transmission substation switch house PSPs, [redacted] of which resided within a generation plant perimeter. These PSPs housed [redacted] Medium Impact BES Cyber Systems also classified as [redacted] BES Cyber Assets, [redacted] Protected Cyber Assets (PCAs), [redacted] Electronic Access Control or Monitoring Systems and [redacted] PACSs.

67. On January 31, 2017, [redacted] discovered the issue when the employee could not gain access to a substation PSP with the new badge as expected. [redacted] corporate security updated the CIP PACS system to reflect the new badge the same day.

68. On April 27, 2017, [redacted] completed an enterprise extent-of-condition assessment and found no additional instances of not updating CIP PACS records associated with lost badges.

69. SERC determined that the root cause of this violation was a lack of training for the individual who issued the replacement badge, as well as a lack of internal controls for badge management and assignment.

70. This violation started on December 5, 2016, when [redacted] did not deactivate a lost CIP PSP access badge, and ended January 31, 2017, when [redacted] deactivated PSP access from the lost access badge.

71. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[8] By not restricting PSP access to only authorized individuals, there was a potential for adverse consequences if malicious actors were to gain operational control of or the ability to reconfigure BES Cyber Assets and Systems. However, in this instance, the lost badge allowed physical, but not electronic or Interactive Remote Access to any BES Cyber Assets. All [redacted] substation switch houses had additional layers of defense, including perimeter fences with locked gates with access only by use of a physical key and camera surveillance at all times. [redacted] switch houses were within the bounds of

[8] According to the CIP-006-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

generating plant perimeters and actively guarded by security personnel at all times. [redacted] confirmed that the lost badge was not used to gain or attempt to gain access to the [redacted] PSPs.

Mitigating Actions for SERC2017017286

72. On June 26, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-006-6 R1, Part 1.2. *See* Mitigation Plan for SERC2017017286. On February 18, 2019, SERC accepted the Mitigation Plan.

73. To mitigate this violation [redacted]:

i. reviewed badge logs to confirm the lost badge was not used or attempted to be used to gain access after being reported lost and while remaining active in the CIP PACS badging system;

ii. [redacted] improved the daily review process by creating a daily reconciliation report that lists employee badge changes in all of the operating companies' non-CIP badge systems and [redacted] generation plants and compared those badge numbers to a list of active CIP PACS badge numbers to identify any discrepancies and make updates;

iii. [redacted] worked with each operating company badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and made updates where necessary; and

iv. to determine the extent of condition, [redacted] worked with each operating company badge office to perform a badge system records reconciliation review to ensure there were no additional lost badges updated in a non-CIP badge system that remained active in the CIP PACS badging system.

74. On June 26, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of May 1, 2017. *See* Certification of Mitigation Plan Completion for SERC2017017286.

F. CIP-006-6 R2 (SERC2017018440 and SERC2017018441)

75. CIP-006-6 requires the management of physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

76. CIP-006-6 R2 states in relevant part:

> **R2.** Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.

P2.1. Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.

P2.2. Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.

Description of Alleged Violation and Risk Assessment for SERC2017018440

77. On October 6, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in noncompliance with CIP-006-6 R2. *See* Self-Report for SERC2017018440. [redacted] had one instance where it failed to continuously escort a visitor while inside a Physical Security Perimeter (PSP) (Part 2.1) and four instances where [redacted] failed to document all required information in its logbooks for visitors who accessed [redacted] PSPs (Part 2.2).

78. On February 1, 2017, [redacted] failed to capture the exit time of a visitor in the manual visitor log book (Part 2.2).

79. On March 21, 2017, members of the [redacted] discovered this missing information when they were on-site at a transmission substation PSP.

80. On June 7, 2017, [redacted] transmission compliance reported this failure to [redacted] operations compliance. After investigating the visit, including reviewing video surveillance and access records from the Physical Access Control Systems (PACS), [redacted] concluded that the escort continuously accompanied the visitor at all times.

81. On July 18, 2017, [redacted] completed an extent-of-condition assessment using a CIP internal controls sampling approach. [redacted] reviewed a random sample of [redacted] out of a total of [redacted] PSP visitor log books across the [redacted] footprint and identified no additional [redacted] logging issues. However, [redacted] identified two [redacted] Control Center logging oversights, which [redacted] self-reported separately under NERC Violation ID: SERC2017018441.

82. However, on July 14, 2017, while performing a biennial CIP-006-6 R3 compliance review of applicable substations, [redacted] discovered the following additional instances of noncompliance with CIP-006-6 R2.

83. On June 7, 2017, three visitors not authorized for unescorted physical access entered a PSP beginning 8:24 a.m. The last visitor left at approximately 5:00 p.m.

However, in all cases [redacted] did not manually log the visitors' PSP entry or exit (Part 2.2).

84. While [redacted] continuously escorted two of the three visitors, it left one of the three visitors unescorted in the transmission substation PSP for 5 hours and 22 minutes (Part 2.1). The unescorted visitor was a generator vendor, on-site for a total of 6 hours and 42 minutes to participate in capacity and heat rate testing. The visitor took readings every 10 minutes between approximately 9 a.m. and 5 p.m. During the periods the visitor was unescorted, the escort remained in the substation yard.

85. For all instances, [redacted] performed a technical assessment to ascertain whether there were any attempts to access BES Cyber Assets (BCAs) or whether baseline configurations changed. [redacted] discovered no irregularities.

86. The [redacted] substations involved contained [redacted] medium impact BES Cyber Systems also classified as BCAs, [redacted] Protected Cyber Assets (PCAs), [redacted] Electronic Access Control or Monitoring System (EAMS), and [redacted] PACS Cyber Assets.

87. The root cause was insufficient training related to the visitor control program.

88. This violation started on February 1, 2017, when [redacted] failed to log the exit time for the first visitor, and ended June 7, 2017, when [redacted] failed to log the exit time for the last visitor.

89. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[9] By not escorting visitors and logging PSP ingress and egress times, [redacted] afforded an opportunity for potential malicious actors to access and modify or compromise the operation of BCSs, with a reduced level of situational awareness for investigating incidents in the wake of grid disturbances. However, [redacted] failed to escort only one visitor. [redacted] confirmed PSP entry and exit times and visitor actions by reviewing badge records of the escort along with video surveillance footage. The unescorted visitor did not possess electronic access credentials to any BCSs or Cyber Assets.

Mitigating Actions for SERC2017018440

90. On October 6, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-006-6 R2, Parts 2.1 and 2.2. *See* Mitigation Plan for SERC2017018440. On February 18, 2019, SERC accepted the Mitigation Plan.

91. To mitigate this violation, [redacted]

[9] According to the CIP-006-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

i. conducted retraining sessions with the responsible escort to review the documented visitor control program and reinforce proper escort logging responsibilities;

ii. [redacted] and affiliated operating company transmission business units performed an extent-of-condition review of ninety days' worth of a random sample of PSPs to determine if additional PSP visitor log book issues existed;

iii. transmission maintenance general manager conducted a safety stand down review session with their direct reports to emphasize the importance of compliance with the CIP visitor control program;

iv. crew foremen conducted a review session with their direct reports, including the employee involved in the instant noncompliance, to emphasize the importance of compliance with the CIP visitor control program;

v. notified managers/supervisors that have direct reports with [redacted] CIP substation unescorted badge access and instruct them on the NERC CIP visitor escort requirements;

vi. [redacted] conducted and completed its biennial review of substation PSPs and reported back any additional log book issues found;

vii. produced and disseminated additional reinforcement on the documented CIP visitor control program in the Q3 CIP cyber security awareness newsletter on proper escorting and logging responsibilities;

viii. reviewed before and after baseline configurations of devices in the substation to verify that while the visitor was unescorted, they did not attempt to access and did not make any changes to any CIP systems while in the substation;

ix. completed a CVA for all applicable CIP systems within the substation to confirm no unauthorized changes were made to devices within the substation; and

x. developed signage and added it to the [redacted] medium substation PSPs providing reinforcement to on-site personnel on visitor escorting and logging responsibilities.

92. On January 23, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of January 23, 2018. *See* Certification of Mitigation Plan Completion for SERC2017018440.

Description of Alleged Violation and Risk Assessment for SERC2017018441

93. On October 6, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-006-6 R2. *See* Self-Report for SERC2017018441. [redacted] had three instances where it failed to continuously escort visitors while inside PSPs (Part 2.1), and two instances where [redacted] failed to

document all the required information in its logbooks for visitors who access [redacted] PSPs (Part 2.2).

94. On February 15, 2018, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in noncompliance with CIP-006-6 R2, Part 2.2. *See* Self-Report for SERC2017018441. [redacted] had one instance where it did not log the time of a visitor's exit from a PSP. SERC later determined that this instance was related to the initial October 6, 2017 Self-Report and decided to treat the subsequent Self-Report as an expansion of scope.[10]

95. On April 20, 2017, a [redacted] escort omitted the name of a contract cleaning visitor from the manual log book. The cleaning visitor arrived at the [redacted] Control Center [redacted] at 8:45 p.m. and exited at 9:14 p.m. On the same day, the same [redacted] escort omitted the time of exit of a different contract cleaning visitor from the manual log book. The second cleaning visitor entered the [redacted] at 9:14 p.m. [redacted] used its PACS records to determine the second cleaning visitor left at 9:23 p.m. [redacted] reviewed recorded video and confirmed that in both instances, the [redacted] escort continuously escorted the visitors.

96. These instances started on April 20, 2017 at 8:45 p.m., when [redacted] failed to log the first visitor's name, and ended April 20, 2017 at 9:23 p.m., when the escort and the second visitor exited the [redacted]

97. On July 18, 2017, [redacted] identified these two PSP manual logging deficiencies at the [redacted], while conducting an extent-of-condition assessment associated with an [redacted] violation, NERC Violation ID: SERC2017018440. For the extent of condition assessment for NERC Violation ID: SERC2017018440, [redacted] reviewed a random sample of [redacted] PSP visitor log books out of a total of [redacted] across the [redacted] footprint and only identified these [redacted] logging oversights.

98. While investigating and mitigating the first two log book deficiencies, [redacted] discovered the following additional two instances where it did not continuously escort visitors while in the [redacted] PSP.

99. On August 2, 2017, a [redacted] escort left a visitor alone in the escort's office, which was located within the [redacted] PSP. The visitor was a co-op student conducting required work activities. Another [redacted] employee discovered the unescorted visitor and immediately escorted the visitor out of the [redacted] PSP. The student visitor entered the PSP at 7:26 a.m. The escort left the office to visit the restroom and was gone for less than five minutes.

[10] This self-reported noncompliance was assigned NERC Tracking Number SERC2018019199 but was administratively dismissed and consolidated with SERC2017018441 on March 8, 2019.

100. This instance started on August 2, 2017, when the escort left the visitor alone, and ended on August 2, 2017, about five minutes later, when another employee escorted the visitor out of the PSP.

101. On August 10, 2017, a [redacted] facilities contractor, who was an authorized escort, did not continuously escort a contract-cleaning visitor while the visitor cleaned and restocked the [redacted] PSP breakroom. At approximately 7:00 p.m., a [redacted] employee noticed the visitor standing alone in the breakroom and immediately assumed escort responsibility and took the visitor to find the original escort. Based on the manual log entry time of 6:55 p.m., [redacted] determined the visitor was unescorted for approximately five minutes.

102. This instance started on August 10, 2017, when the escort left the visitor alone, and ended on August 10, 2017, about five minutes later, when another employee took over escorting the visitor.

103. The [redacted] at issue housed [redacted] BCAs within a High Impact BCS, [redacted] PCAs, [redacted] EACMS Cyber Assets, and [redacted] PACS Cyber Asset.

104. On December 19, 2017 at 7:47 p.m., an [redacted] facility control operator escorted an [redacted] contractor visitor into the [redacted] energy management system (EMS) office area PSP, which included [redacted] high impact BES Cyber Systems also classified as BES Cyber Assets. The purpose of the visit was to access a fire alarm panel for fire alarm testing that was taking place in the [redacted] corporate headquarters that evening. While the manual log entry upon entering the PSP was complete, [redacted] omitted the time of exit. [redacted] later reviewed PACS records, which reflected the exit but not entrance of the escort and visitor, and determined that the visitor exited the PSP at 7:49 p.m. The escort stayed with the visitor at all times while within the PSP.

105. This instance started and ended on December 19, 2017 at 7:49 p.m., when [redacted] did not log the visitor's time of exit from the PSP.

106. On January 22, 2018, [redacted] EMS compliance discovered the missing exit time for the [redacted] visitor during a sporadic spot check of the visitor log book used in the [redacted] EMS PSP.

107. [redacted] conducted an extent-of-condition assessment by reviewing other [redacted] facility control operators activities related to fire alarm testing during the evening of December 19, 2017. No visitor access of other PSPs occurred that evening.

108. The root cause of this violation was the absence of sufficient training related to the visitor control program.

109. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[11] By not consistently escorting visitors and following manual logging procedures, [redacted] afforded an opportunity to potential malicious actors to access and modify or compromise the operation of BCSs, with a reduced level of situational awareness in the event of the need to investigate incidents of grid disturbances. However, [redacted] only left the two visitors unescorted for approximately 10 minutes in total. Further, the visitors were only in areas of the PSP that did not contain any BCSs or Cyber Assets. For the three instances of manual logging deficiencies, [redacted] used badge access records and video surveillance to confirm the identity of visitors, verify continual escort, and verify entry and exit times. Further, the [redacted] EMS PSP visitor had a current personnel risk assessment and had completed cyber security training and [redacted] later authorized the individual for unescorted physical access to a different PSP.

Mitigating Actions for SERC2017018441

110. On February 7, 2019, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-006-6 R2, Parts 2.1 & 2.2, including all instances identified in the Self-Reports and the subsequent expansion of scope. *See* Mitigation Plan for SERC2017018441. On March 7, 2019, SERC accepted the Mitigation Plan.

111. To mitigate this violation, [redacted]:

i. [redacted] and each [redacted] and operating company business unit performed an extent-of-condition review of a random sample of PSP visitor log books to determine if any additional log book issues existed;
ii. disseminated additional reinforcement on the entity's CIP visitor control program in the CIP quarterly awareness newsletter on proper escorting and logging responsibilities;
iii. coordinated in-person retraining on CIP visitor control responsibilities for personnel working in the [redacted] with authorized unescorted physical access to the [redacted]
iv. coordinated in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] corporate facilities and personnel working for the contract cleaning vendor with authorized unescorted physical access to the [redacted];
v. [redacted] corporate facilities performed an extent-of-condition review to determine if any other [redacted]

[11] According to the CIP-006-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

corporate facilities employees escorted any contractors into a PSP to perform fire alarm testing on the evening of December 19, 2017, to ensure all visitors, if any, were properly logged in PSP visitor log books;

vi. administered required in-person refresher training on CIP visitor control with the [redacted] facility operator that was responsible for escorting the contractor, covering visitor log book requirements and escort responsibilities when escorting visitors within a PSP; and

vii. conducted in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] corporate facilities.

112. On April 18, 2019, [redacted] certified to SERC that it completed the Mitigation Plan as of February 23, 2018. *See* Certification of Mitigation Plan Completion for SERC2017018441.

G. CIP-007-6 R1, Part 1.1 (SERC2016016492)

113. CIP-007-6 ensures that Responsible Entities define select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

114. CIP-007-6 R1 states in relevant part:

> **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.
>
> **P1.1.** Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

Description of Alleged Violation and Risk Assessment for SERC2016016492

115. On November 3, 2016, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in noncompliance with CIP-007-6 R1, Part 1.1. *See* Self-Report for SERC2016016492. [redacted] had one instance where it enabled two unneeded logical network accessible ports.

116. On July 1, 2016, [redacted] commissioned an Electronic Access Control or Monitoring System (EACMS). Prior to commissioning the EACMS, [redacted] had determined that it did not require two ports, but [redacted] failed to disable the two ports.

117. The scope of affected Facilities included the Cyber Assets associated with the EACMS and Physical Access Controls System (PACS) for all [redacted] substations containing medium impact BES Cyber Systems [redacted].

118. On July 27, 2016, [redacted] discovered these unneeded open ports while performing a security controls verification after commissioning the EACMS. On August 2, 2016, [redacted] disabled the [redacted] unneeded ports.

119. [redacted] conducted an extent-of-condition review of all assets managed by the new compliance team that had responsibility for compliance with the CIP Reliability Standards and Requirements in a limited number of sites and applications (i.e., substations and specifically EACMS and PACS). [redacted] found no additional instances of enabled ports that were unneeded.

120. The root cause of this violation was the absence of sufficient training to ensure successful execution of commissioning-related procedures for disabling unneeded ports.

121. This violation started on July 1, 2016, when [redacted] commissioned the EACMS, and ended on August 2, 2016, when [redacted] disabled the unneeded ports.

122. This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS.[12] [redacted] failure to disable unneeded ports presented an increased potential for discovery and exploitation by intruders, allowing them to gain operational control of cyber assets and grid facilities. However, ports erroneously enabled were secure communications-related services which [redacted] did not utilize. The affected Cyber Assets were not internet facing and were within a dedicated and protected domain, which had dedicated firewalls configured to maintain segregation of any CIP environments from any corporate data. In addition, a newly formed CIP team was responsible for this error. [redacted] created the new team to help manage access control and access management for medium impact substations under CIP Version 5.

Mitigating Actions for SERC2016016492

123. On November 3, 2016, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R1, Part 1.1. *See* Mitigation Plan for SERC2016016492. On February 18, 2019, SERC accepted the Mitigation Plan.

124. To mitigate this violation, [redacted]:

i. disabled the unneeded service on the device;

[12] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "High" VSL.

ii. performed a review of all its CIP Cyber System baseline documentation and verified those ports and services documented in the baselines were the only ones enabled;

iii. conducted a review session of the applicable [redacted] IT work practices addressing CIP-007-6 R1.1 and retrained department personnel on confirming only logical network accessible ports which are needed are enabled; and

iv. required department personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedure going forward.

125. On January 19, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of December 7, 2016. *See* Certification of Mitigation Plan Completion for SERC2016016492.

H. CIP-007-6 R2, Part 2.3 (SERC2017018467)

126. CIP-007-6 ensures that Responsible Entities define select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

127. CIP-007-6 R2 states in relevant part:

> **R2.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2-Security Patch Management.
>
> **P2.1.** A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
>
> **P2.2** At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.
>
> **P2.3.** For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:
>
> - Apply the applicable patches; or
> - Create a dated mitigation plan; or
> - Revise an existing mitigation plan.

Attachment A

Description of Alleged Violation and Risk Assessment for SERC2017018467

128. On October 11, 2017, [redacted] submitted a Self-Report to [redacted] stating that, as a [redacted], it was in violation of CIP-007-6 R2, Part 2.3. *See* Self-Report for SERC2017018467. [redacted] had one instance where it did not deploy an applicable patch within 35 calendar days of completion of the patch evaluation.

129. On July 11, 2017, [redacted] evaluated security patches and determined it did not deploy one applicable patch correctly onto [redacted] Electronic Access Control or Monitoring System (EACMS) servers at a [redacted] substation containing medium impact BES Cyber Systems until September 8, 2017, 63 days after the evaluation completion. The missed patch addressed security vulnerabilities, security updates on unsupported hardware not being scanned for, and issues with printing and using a mouse.

130. On September 7, 2017, [redacted] discovered the unapplied assessed patch during a review of patches deployed by the application during July 2017.

131. On September 13, 2017, [redacted] concluded its extent-of-condition assessment to verify [redacted] and all [redacted] operating companies had applied all applicable patches to the endpoints within the required 35 calendar day timeframe and [redacted] did not find any additional discrepancies.

132. The root cause of this violation was deficient procedures that lacked details related to roles and responsibilities and related internal controls.

133. This violation started on August 15, 2017, the day after when [redacted] should have applied the security patch, and ended on September 8, 2017, when [redacted] applied the patch.

134. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[13] By not timely applying a security patch, there was a potential for exploitation of transient vulnerabilities, allowing intruders to degrade or disable EACMS monitoring and alerting processes, potentially facilitating malicious control of Facilities and degradation of grid security. However, [redacted] only missed the deadline for applying the patch by 24 days. [redacted] only missed applying the patch on [redacted] of [redacted] Cyber Assets (1.15%) that needed this patch. In addition, [redacted] protected the EACMS with device whitelisting services.

[13] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Moderate" VSL.

135. On October 11, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R2, Part 2.3. *See* Mitigation for SERC2017018467. On February 18, 2019, SERC accepted the Mitigation Plan.

136. To mitigate this violation, [redacted]

i. applied the missed patch to the [redacted] servers;
ii. completed a review and verified that all applicable endpoints were patched and that all patch levels are current;
iii. made improvements to the documented substation system access control management work practice, to include defined responsibilities for the administrators responsible for patching at [redacted] and [redacted]; and
iv. conducted a review/training session with administrators responsible for patching on applicable changes to the documented substation system access control management work practice addressing CIP-007-6 R2.3.

137. On October 11, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of October 11, 2017. *See* Certification of Mitigation Plan Completion for SERC2017018467.

I. CIP-007-6 R3, Part 3.1 (SERC2017017236)

138. CIP-007-6 ensures that Responsible Entities define select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

139. CIP-007-6 R3 states in relevant part:

> **R3.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.
>
> **P3.1.** Deploy method(s) to deter, detect, or prevent malicious code.

Description of Alleged Violation and Risk Assessment for SERC2017017236

140. On March 16, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-007-6 R3, Part 3.1. *See* Self-Report for SERC2017017236. [redacted] had one instance where it did not deploy a method to deter, detect, or prevent malicious code.

141. On October 2, 2016, a process to enforce whitelisting stopped working properly on [redacted] Electronic Access Control or Monitoring System (EACMS) servers at [redacted]

substations and [redacted] substations. [redacted] used the method of whitelisting to deter, detect, or prevent malicious code. The [redacted] EACMS servers provided access to [redacted] medium impact BES Cyber Systems also classified as [redacted] BES Cyber Assets, [redacted] Protected Cyber Assets, and [redacted] EACMS.

142. On December 5, 2016, while verifying security controls following a change to the [redacted] EACMS servers, [redacted] discovered this noncompliance.

143. On March 14, 2017, [redacted] successfully completed deployment of policy file refreshes to the [redacted] servers and verified whitelisting worked properly.

144. To determine the extent-of-condition, [redacted] conducted a [redacted] enterprise-wide check of all other servers of the same brand with the same whitelisting process similarly employed, and confirmed all were working correctly.

145. The root cause of this violation was faulty software, which caused the whistleblowing process to stop working.

146. This violation started October 2, 2016, when the whitelisting process stopped working, and ended February 7, 2017, when [redacted] reestablished the whitelisting process.

147. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[14] By not deterring, detecting, or preventing malicious code on an EACMS, there was a potential for intruders to compromise monitoring, event logging and alert issuance. Thus, there would be a greater potential for intruders to manipulate BES Cyber Systems and BPS facilities and affect grid security. However, the EACMS still functioned, although the loss of whitelisting made it less secure. This issue affected only a portion of EACMS whitelisting, [redacted] of [redacted] similarly configured servers, and not whitelisting on other applicable systems. The introduction of malicious code to the EACMS servers would have required using IRA or PSP access. Both methods of access required authorization and credentials. For IRA, [redacted] required the use of an Intermediate System and multi-factor authentication.

Mitigating Actions for SERC2017017236

148. On July 10, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R3, Part 3.1. *See* Mitigation Plan for SERC2017017236. On February 18, 2019, SERC accepted the Mitigation Plan.

149. To mitigate this violation, [redacted]:

[14] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

i. completed an extent of condition review of the functionality of the involved whitelisting on all other servers of the same brand with the same whitelisting process similarly employed to confirm whitelisting is enabled and properly enforcing device whitelists for [redacted] and [redacted] devices;

ii. disabled IRA capability to the involved servers to temporarily harden the devices and prevent external remote access until resolution with the vendor can be achieved;

iii. worked with [redacted] IT and the contracted vendor to confirm that whitelisting rules were re-enabled and functioning properly to deter, detect, and prevent malicious code on the affected devices; and

iv. reviewed substation work practices and determined if any updates or corrections could be made to help with troubleshooting and/or identifying this issue in a timelier manner.

150. On July 10, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of March 15, 2017. *See* Certification of Mitigation Plan for SERC2017017236.

J. CIP-007-3a R5 (SERC2017016832)

151. CIP-007-3a Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the ESPs.

152. CIP-007-3a R5 states in relevant part:

> **R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimizes the risk of unauthorized system access.
>
> **R5.1.** The Responsible Entity shall 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.
>
> **R5.1.1.** The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.
>
> **R5.1.2.** The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

Description of Alleged Violation and Risk Assessment for SERC2017016832

153. On January 25, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-007-3a R5, R5.2 and R5.3. *See* Self-Report for SERC2017016832. [redacted] did not change passwords for [redacted] administrator, shared, and other generic accounts prior to commissioning (R5.2.1) and did not change passwords for such accounts annually (R5.3.3).

154. Between May 31, 2011 and October 7, 2016, [redacted] commissioned an additional [redacted] terminal servers, but did not change the passwords on them prior to putting them into service and did not change the passwords annually

thereafter. On May 4, 2015, [redacted] last changed passwords on [redacted] EMS-related [redacted] terminal servers, but did not change the passwords annually thereafter.

155. [redacted] designated all [redacted] terminal servers as Critical Cyber Assets (CCAs) under CIP Version 3. Furthermore, [redacted] documented technical and procedural controls requiring changing passwords on shared accounts at least [redacted] a year. Since [redacted] had designated all [redacted] servers as CCAs under CIP Version 3, [redacted] was required to change passwords at least annually. However, [redacted] did not change passwords at least annually on any of the [redacted] terminal servers.

156. On August 31, 2016, [redacted] discovered that it failed to change passwords on the [redacted] EMS-related servers annually. While investigating into whether it failed to annually change the passwords on any other similar [redacted] servers, [redacted] discovered its failure to change the passwords on the [redacted] servers prior to putting them into service. On November 22, 2016, [redacted] completed changing passwords on all [redacted] terminal servers.

157. [redacted] performed an extent-of-condition assessment by reviewing whether it changed passwords of all shared accounts on all applicable EMS devices at least once every six months, as required by its documented procedures, and found no additional instances of noncompliance.

158. The root cause of this violation was a combination of lack of adequate training and internal controls to ensure the proper documentation of inventory and password status.

159. This violation started on May 31, 2011, when [redacted] started commissioning servers without first changing the passwords on them and ended on November 22, 2016, when [redacted] changed the last overdue password.

160. This violation posed a serious risk to the reliability of the BPS.[15] By not changing passwords on [redacted] CCAs for nearly five years, there was an extended window of heightened risk where malicious actors could have discovered and exploited unchanged passwords and interfered with grid security. However, the communication paths serviced by the terminal servers employed dual redundancy with automatic failover and continuous monitoring. Logging on to the affected CCAs required two-factor authentication.

[15] CIP-007-3a R5.2.1 and R5.3.3 have VRFs of "Medium" pursuant to the VRF Matrix. According to the VSL Matrix, this violation warranted a "Severe" VSL.

Attachment A

Mitigating Actions for SERC2017016832

161. On February 8, 2019, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-3a R5; R5.2.1 and R5.3.3. *See* Mitigation Plan for SERC2017016832. On March 5, 2019, SERC accepted the Mitigation Plan.

162. To mitigate this violation, [redacted]

i. trained EMS employees on the EMS protected password repository user guide process for managing [redacted] passwords and password changes in the protected password repository application;
ii. changed all shared user account passwords on the [redacted] then current, EMS [redacted] devices;
iii. edited the electronic access work practice to include a reference to the EMS protected password repository user guide used for password management of [redacted] devices going forward using the EMS protected password repository application; and
iv. transitioned shared account password storage and management for the [redacted] devices to the EMS protected password repository application to automate password changes in the event of personnel changes.

163. On February 8, 2019, [redacted] certified to SERC that it completed the Mitigation Plan as of February 1, 2017. *See* Certification of Mitigation Plan Completion for SERC2017016832.

K. CIP-007-6 R5 (SERC2017018246, SERC2018019200, SERC2017018548, and SERC2016016339)

164. CIP-007-6 ensures that Responsible Entities define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter.

165. CIP-007-6 R5 states:

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.

P5.1. Have a method(s) to enforce authentication of interactive user access, where technically feasible.

P5.2. Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

P5.3. Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

P5.4. Change known default passwords, per Cyber Asset capability.

P5.5. For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.

P5.6. Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

P5.7. Where technically feasible, either:

- Limit the number of unsuccessful authentication attempts; or
- Generate alerts after a threshold of unsuccessful authentication attempts.

Description of Alleged Violation and Risk Assessment for SERC2017018246

166. On August 24, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in violation of CIP-007-6 R5, Part 5.1. *See* Self-Report for SERC2017018246. [redacted] had two instances where it did not authenticate interactive user access to PACS Cyber Assets where technically feasible.

167. On April 18, 2017, a [redacted] employee errantly added [redacted] unauthorized domain groups to [redacted] Physical Access Control System (PACS) workstations, thus permitting another employee to log into the workstations, check for software issues, and update antivirus software. [redacted] did not authorize the support employee to conduct interactive user access on the PACS workstations. The addition of the access domains permitted multiple unauthorized persons to utilize interactive user access. The domain group policy objects settings for these assets failed to properly enforce the domain policy to restrict access to only [redacted] authorized groups.

168. On April 21, 2017, during a sporadic review of access logs on the [redacted] PACS workstations, [redacted] discovered its previous error in access provisioning.

169. On April 24, 2017, [redacted] remedied the access provisioning issue when it changed domain policy ordering, then forced a policy refresh and reboot on the [redacted] PACS workstations, thereby restoring the correct intended enforcement of authentication of interactive user access.

170. In another instance, sometime prior to July 1, 2016, [redacted] had overridden a limiting access control through a misconfigured higher-level control, thus allowing unintended groups of unauthorized users' remote access to [redacted] PACS workstations.

171. On August 15, 2017, while conducting a review of access attempts on the [redacted] PACS workstations as part of mitigation for the first instance, [redacted] employees discovered this error. On the same day, [redacted] remedied this error when it blocked the higher-level control, removed all existing groups, and added back only the intended group.

172. The scope of affected Facilities included all Facilities protected by [redacted] Physical Security Perimeters (PSPs), including [redacted] control centers and backup control centers, [redacted] data centers, [redacted] transmission substations, [redacted] high impact BES Cyber Assets/[redacted] BES Cyber Systems (BCAs/BCSs) and associated Electronic Access Control or Monitoring Systems (EACMS) Cyber Assets and Protected Cyber Assets (PCAs), [redacted] medium impact BCAs/BCSs and associated EACMSs, PCAs, and PACS Cyber Assets.

173. [redacted] conducted an extent-of-condition assessment to ensure that it had not made the same error on other PACS Cyber Assets. The PACS assets were the only assets that resided on the corporate domain and all other systems were segregated off onto their own domains and would not have been subject to this type of failure. [redacted] found no additional issues.

174. The root causes of this violation were a lack of managerial oversight, a lack of internal controls, and a lack of adequate training on properly implementing the internal controls.

175. This violation started on July 1, 2016, when [redacted] commissioned [redacted] PACS workstations with misconfigured access controls allowing groups of unauthorized users' remote access to them, and ended August 15, 2017, when [redacted] last restricted access to only authorized users.

176. SERC determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[16] By not enforcing authentication to only authorized users, there was a potential for bad actors to access PACS monitoring workstations. However, the access granted was limited to company IT administrators authorized for interactive user CIP access to other domains. Access

[16] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

was limited to only the operating system and non-PACS installed applications on the workstations. Access to the application software used to monitor, add, delete or modify PACS access controls required additional authentication credentials and access controls afforded only to authorized users. [redacted] configured all affected workstations without internet-facing applications and it continuously monitored PACS systems, primary and separately located backup, for losses in functionality.

Mitigating Actions for SERC2017018246

177. On July 1, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R5, Part 5.1. *See* Mitigation Plan for SERC2017018246. On February 18, 2019, SERC accepted the Mitigation Plan.

178. To mitigate this violation, [redacted]

i. Modified, as necessary, the group policy object (GPO) administrator group policy preferences for the workstations to reapply existing domain controls to enforce removal of errant accounts and allow only the designated and authorized groups;
ii. implemented a more frequent (weekly) review of PACS workstations and servers local administrator accounts until it completed milestone four;
iii. modified, as necessary, related security settings on higher level governing GPO and updated existing groups control on remote desktop users group policy preferences to reapply the intended governing GPOs and to enforce the removal of errant accounts to allow only the designated and authorized groups;
iv. implemented its existing system access control application's logging and alerting on any group changes to GPO settings on PACS workstations; and
v. realigned these PACS workstations on the corporate domain into their own organizational unit to further restrict GPO changes.

179. On July 12, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of January 11, 2018. *See* Certification of Mitigation Plan Completion for SERC2017018246.

Description of Alleged Violation and Risk Assessment for SERC2018019200

180. On February 16, 2018, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in violation of CIP-007-6 R5. *See* Self-Report for SERC2018019200. SERC later determined [redacted] was specifically in violation of CIP-007-6 R5, Parts 5.2 and 5.4. [redacted] did not change known default passwords, per Cyber Asset capability, for [redacted] EACMS servers (Part 5.4). Also, for [redacted] of the servers,

[redacted] did not identify and inventory all known enabled default generic account types (Part 5.2).

181. On July 1, 2016, [redacted] commissioned [redacted] EACMS servers without changing a user account default password on them.

182. On December 18, 2017, during a security controls check prior to upgrading software on [redacted] of the [redacted] servers, [redacted] IT employees discovered the default passwords.

183. On December 20, 2017, [redacted] changed the [redacted] default passwords.

184. On January 5, 2018, during a subsequent extent-of-condition assessment, [redacted] employees discovered the two additional instances of an identical nature affecting [redacted] additional servers. For the [redacted] additional servers, [redacted] also had not identified and inventoried the accounts, classified as default generic user accounts.

185. On January 8, 2018, [redacted] changed the default passwords and identified and inventoried the accounts for the [redacted] servers.

186. [redacted] classified the [redacted] security event-monitoring servers involved as EACMS, which affected all [redacted] of [redacted] operating companies' substations ESPs containing medium impact BCSs [redacted].

187. On May 3, 2018, as part of its mitigation for this noncompliance, [redacted] completed an extent-of-condition assessment by reviewing documentation for CIP-007 R5, Parts 5.2, 5.3, and 5.4 associated with all CIP Cyber Systems managed by the team involved in this noncompliance. During the extent-of-condition review, [redacted] discovered it did not identify and document shared accounts on [redacted] PACS and [redacted] administrator accounts on [redacted] servers hosting [redacted]. [redacted] also discovered it did not document [redacted] accounts on [redacted] servers used for EACMS logging.

188. The root cause of this violation was incomplete and insufficient procedures related to the deployment of newly commissioned Cyber Assets.

189. This violation started on July 1, 2016, when [redacted] commissioned servers without changing default passwords and without inventorying default accounts, and ended on January 8, 2018, when [redacted] changed passwords and inventoried default accounts.

190. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[17] By not changing account default passwords and not inventorying accounts, malicious intruders could have rendered transmission substation EACMSs inoperable or unavailable, thus potentially opening a gateway for the introduction of malicious code or configuration changes to BCSs employed in monitoring and operating transmission substations. However, in this instance EACMSs managed firewalls and Intermediate Systems protecting BCSs and PCAs, which were unaffected. [redacted] housed the involved servers in access controlled, continuously monitored PSPs, and segregated the servers in a separate, secure domain.

Mitigating Actions for SERC2018019200

191. On July 23, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R5, Parts 5.2 and 5.4. *See* Mitigation Plan for SERC2018019200. On February 18, 2019, SERC accepted the Mitigation Plan.

192. To mitigate this violation, [redacted]

i. changed the default password on the involved connector devices;
ii. conducted a review session with the personnel responsible for changing the involved account password and the importance of compliance with the CIP program;
iii. changed the involved default password on the involved system access control application [redacted] devices;
iv. updated the CIP-007 R5.2 documentation for the [redacted] system access control application connecter servers and the [redacted] system access control application [redacted] servers;
v. modified the default, generic and shared accounts work practice to provide more specific instruction for account identification and password change requirements;
vi. conducted reinforcement counselling with personnel responsible for account management of the involved CIP assets; and
vii. performed a review of all CIP Cyber Systems and associated CIP-007 R5 documentation managed by the involved group to ensure all accounts are identified, inventoried, and meet the CIP-007 R5.2, R5.3, and R5.4 requirements.

193. On July 23, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of May 18, 2018. *See* Certification of Mitigation Plan Completion for SERC2018019200.

[17] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

Attachment A

Description of Alleged Violation and Risk Assessment for SERC2017018548

194. On October 30, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-007-6 R5, Part 5.4. *See* Self-Report for SERC2017018548, [redacted] did not change known default passwords for two accounts on a RTU.

195. On May 25, 2017, [redacted] commissioned a RTU without changing its administrator account default password and without changing the password on its default service account. This non-compliance affected a single substation and a single BCS which was also a BCA. [redacted]

196. On June 12, 2017, while conducting a post-commissioning inventory review of relevant data, [redacted] discovered this violation. On November 8, 2017, [redacted] conducted an enterprise-wide review and assessment of all BCAs commissioned since July 1, 2016, and identified no additional instances.

197. The root cause of this violation was the absence of adequate training in commissioning procedures.

198. This violation started on May 25, 2017, when [redacted] commissioned the RTU for service without changing default passwords, and ended on June 13, 2017, when [redacted] renamed and changed the default password for the administrator account and deleted the service account.

199. This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS.[18] By not changing known default passwords, there was a potential for hackers to gain control of a substation RTU and BPS facilities, and cause grid instability. [redacted] protected the RTU behind a firewall within an ESP and housed it within a PSP, and monitored both at all times. [redacted] discovered this issue within only three weeks. [redacted] reviewed logs and determined there had been no unauthorized attempts to utilize either of the two accounts or access the PSP.

Mitigating Actions for SERC2017018548

200. On October 30, 2017, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R5, Part 5.4. *See* Mitigation Plan for SERC2017018548. On February 19, 2019, SERC accepted the Mitigation Plan.

201. To mitigate this violation, [redacted]

i. changed the default administration account password and name on the RTU and removed the involved service account;

[18] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

ii. performed an access review of the RTU following commissioning and when the administrator account password and name and service account was changed and/or removed;

iii. added a commissioning task list as an attachment to the substation system access control management work practice as an additional guide for commissioning devices;

iv. completed a review of BCA and PCA devices commissioned at medium impact substations since July 1, 2016, to verify the password requirements were met; and

v. conducted a review and training session with [redacted] and affiliate operating company personnel on the addition of the commissioning task list to the substation system access control management work practice to address CIP-007-6 R5.4.

202. On December 6, 2017, [redacted] certified to SERC that it completed the Mitigation Plan as of December 6, 2017. *See* Certification of Mitigation Plan Completion for SERC2017018548.

Description of Alleged Violation and Risk Assessment for SERC2016016339

203. [redacted] sent [redacted] an ADL notifying it of a Compliance Audit scheduled for [redacted] through [redacted], with the on-site week being the week of [redacted].

204. On [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in noncompliance with CIP-007-6 R5, Part 5.5.1. *See* Self-Report for SERC2016016339. [redacted] had one instance where it did not implement a password length of at least eight characters for an interactive user access account.

205. On July 26, 2016, while conducting a security controls verification review related to a BES Cyber Asset configuration change, [redacted] discovered that the minimum password length setting for domain policy users was set to seven characters, rather than eight characters. Between August 24, 2016 and September 22, 2016, [redacted] conducted a review of user accounts associated with the domain policy, and found one user with a domain password set to less than eight characters. Although a procedural control existed since July 1, 2016 which included a minimum password length of eight, since one user had a password length set to less than eight, [redacted] did not technically or procedurally enforce a password length of at least eight characters. [redacted] failed to update the password length requirement setting in the domain by July 1, 2016.

206. The deficient password requirement setting applied to the Cyber Assets and their associated EACMS and PACS, for all [redacted] substations containing Medium Impact BES Cyber Systems [redacted].

207. [redacted] conducted an extent-of-condition by reviewing all user accounts associated with the involved domain and identified no additional instances of passwords shorter than eight characters.

208. The root cause of this violation was the absence of sufficient training on procedures for password requirements.

209. This violation started on July 1, 2016, when the standard became mandatory and enforceable on [redacted] and ended on August 25, 2016, when [redacted] changed the user's password to comply with the eight character minimum.

210. This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS.[19] By not enforcing password lengths of a least eight characters, [redacted] lessened the security controls of an account, resulting in an increased potential for unauthorized access to Cyber Assets and harm to grid stability. However, documented procedures required a minimum of eight characters and the account had technical controls in place to enforce passwords of at least seven characters. The Cyber Assets affected by this issue did not provide control functionality or facilitate IRA. Malicious intruders would have only had the ability to modify operating system characteristics and related resource allocations.

Mitigating Actions for SERC2016016339

211. On October 6, 2016, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-007-6 R5, Part 5.5.1. *See* Mitigation Plan for SERC2016016339. On February 18, 2019, SERC accepted the Mitigation Plan.

212. To mitigate this violation, [redacted]

i. modified the password policy enforcement tool to technically enforce a password length of eight characters for all domain users where password-only authentication is used;
ii. to determine the extent of condition, completed a review of all [redacted] user's account passwords used on the [redacted] domain to determine if any users were using a password less than 8 characters in length; and
iii. required the one user found using a password less than eight characters in length to change their password based on the updated password policy enforcement tool.

[19] According to the CIP-007-6 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "High" VSL.

213. On October 26, 2016, [redacted] certified to SERC that it completed the Mitigation Plan as of September 22, 2016. *See* Certification of Mitigation Plan Completion for SERC2016016339.

L. CIP-010-2 R1 (SERC2016016321 and SERC2018019106)

214. 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).

215. CIP-010-2 R1 states in relevant part:

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management.

P1.1. Develop a baseline configuration, individually or by group, which shall include the following items:

P1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

P1.1.2. Any commercially available or open-source application software (including version) intentionally installed;

P1.1.3. Any custom software installed;

P1.1.4. Any logical network accessible ports; and

P1.1.5. Any security patches applied.

P1.2. Authorize and document changes that deviate from the existing baseline configuration.

P1.3. For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

P1.4. For a change that deviates from the existing baseline configuration:

P1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

P1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and

P1.4.3. Document the results of the verification.

Attachment A

Description of Alleged Violation and Risk Assessment for SERC2016016321

216. This violation involves 15 instances of noncompliance with CIP-010-2 R1. On [redacted], SERC sent [redacted] an ADL notifying it of a Compliance Audit scheduled for [redacted], with the on-site week being the week of [redacted].

217. On [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it had one instance of noncompliance with CIP-010-2 R1, Part 1.1.4 (Instance 1). *See* Self-Report for SERC2016016321.

218. In the first instance, when transitioning to version 5 of the Standard and Requirement, [redacted] split out the EACMS from its consolidated baselines. During this transition, [redacted] omitted a logical network accessible port in use from its baseline configuration documentation for an Electronic Access Control or Monitoring System (EACMS). [redacted] had included this port in previous versions of the documented baseline configuration, but failed to transfer the data correctly to its July 1, 2016 version. [redacted] used this port to forward device logs to an aggregation server on the exterior of the ESPs. [redacted] should have included this logical network accessible port in the baseline of [redacted] EACMS Cyber Assets in [redacted] substations containing medium impact BES Cyber Systems.

219. [redacted], [redacted] discovered this omission while responding to a data request for the upcoming SERC Compliance Audit.

220. [redacted] conducted an extent-of-condition review of all baseline documentation for substation EACMS across the [redacted] enterprise, including all operating companies, to determine whether it had additional similar discrepancies. During this extent of condition review, [redacted] discovered another port that it omitted from its configuration baselines (P1.1.4) (Instance 2). During the Compliance Audit, SERC identified the same missing port. This port was present on the same EACMS as the first missed port. [redacted] used this port to facilitate whitelisting updates for patch management.

221. Instances 1 and 2 started July 1, 2016, when the Standard and Requirement became mandatory and enforceable on [redacted], and ended on October 6, 2016, when [redacted] corrected the baseline by adding the last of the two missing ports.

222. During the Compliance Audit conducted from [redacted] SERC identified an additional instance of [redacted] failing to include two logical network accessible ports in its baseline configuration (P1.1.4) (Instance 3). *See* PV Audit Summary for SERC2016016321. SERC later determined that this

instance was related to the initial [redacted] Self-Report and decided to treat the subsequent audit finding as an expansion of scope.[20]

223. In this third instance, [redacted] had documented the port range of a different BES Cyber Asset (BCA) as broader in the baseline configuration than the actual port range in use. [redacted] vendor documentation on the required port ranges did not indicate which ports in the ephemeral range were specifically needed and [redacted] did not contact the vendor prior to implementation to confirm or question what was required. As a result, [redacted] had included the entire ephemeral range in its whitelisting. On November 29, 2016, [redacted] contacted the [redacted] vendor to inquire about the required port ranges. On November 30, 2016, the vendor provided written confirmation stating that the port range required for the system was only a limited portion of the ephemeral range.

224. This instance started July 1, 2016, when the Standard and Requirement became mandatory and enforceable on [redacted] and ended on October 7, 2016, when [redacted] corrected the baseline to reflect only the limited portion of the ephemeral range.

225. On [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it had one instance of noncompliance with CIP-010-2 R1, Part 1.1 (Instance 4). *See* Self-Report for SERC2016016321. SERC later determined that this instance was related to the initial [redacted] Self-Report and decided to treat the subsequent Self-Report as an expansion of scope.[21]

226. In this fourth instance, on April 20, 2016, [redacted] upgraded an EACMS associated with High and Medium Impact BES Cyber Systems to a new version that from then on required a certain port. However, [redacted] did not update the baseline configuration documentation accordingly (P1.2). Specifically, a port scan of an EACMS, which hosts [redacted] EACMS-related systems on [redacted] physical servers, revealed an open port not shown as open in the baseline configuration documentation. However, [redacted] required the port.

227. On August 22, 2016, [redacted] discovered this discrepancy while performing a security controls verification prior to installing a security patch. On August 25, 2016, [redacted] updated the baseline configuration as required.

228. This instance started July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended August 25, 2016, when [redacted] updated the baseline.

[20] This audit finding of noncompliance was assigned NERC Tracking Number SERC2016016451, but was administratively dismissed and consolidated with SERC2016016321 on March 8, 2019.
[21] This audit finding of noncompliance was assigned NERC Tracking Number SERC2016016491, but was administratively dismissed and consolidated with SERC2016016321 on March 8, 2019.

229. On May 18, 2017 and on September 15, 2017, [redacted] submitted expansions of scope with 11 additional instances of noncompliance with CIP-010-2 R1, Parts 1.1, 1.2, 1.3, and 1.4 (Instances 5 – 15). *See* Expansion of Scope for SERC2016016321. SERC later determined that these violations were related to the initial September 30, 2016 Self-Report and decided to treat the subsequent Self-Report as an expansion of scope.[22]

230. In the fifth instance, on August 4, 2016, [redacted] applied [redacted] patches to a Physical Access Control System (PACS) server without authorizing and documenting the changes that deviated from the existing baseline configuration (P1.2), and without evaluating, verifying and documenting that required security controls were not adversely affected (P1.4). Due to a procedural oversight, [redacted] wrongly added these patches to a patch deployment group, causing them to be applied early. In addition, [redacted] did not update baseline configuration documentation within 30 calendar days of applying these four security patches (P1.3). [redacted] should have made the update by September 3, 2016, but did not complete it until September 8, 2016.

231. On August 8, 2016, while performing a security controls verification prior to installing patches, [redacted] discovered it had applied these [redacted] patches without performing the change management tasks (P1.1 and P1.4). On August 29, 2016, [redacted] authorized and documented the changes that deviated from the existing baseline configuration and evaluated, verified and documented that required security controls were not adversely affected.

232. This instance started August 4, 2016, when [redacted] applied patches without performing the required tasks, and ended September 8, 2016, when [redacted] updated the baseline documentation.

233. In the sixth instance, on August 15, 2016, [redacted] upgraded software on [redacted] EACMS servers associated with Medium Impact BES Cyber Systems used to support Interactive Remote Access to substations without authorizing and documenting the changes that deviated from the existing baseline configuration (P1.2), and without evaluating, verifying, and documenting that required security controls were not adversely affected (P1.4).

234. On August 26, 2016, [redacted] discovered this error while performing a security controls verification prior to installing a security patch.

[22] The expansion-of-scope instances were assigned NER Violation Number SERC2016016491, but was administratively dismissed and consolidated with SERC2016016321 on March 8, 2019.

235. This instance started on August 15, 2016, when [redacted] upgraded the software without performing the required tasks, and ended September 14, 2016, when [redacted] authorized and documented the changes that deviated from the existing baseline configuration, and evaluated, verified, and documented that required security controls were not adversely affected.

236. In the seventh instance, on August 18, 2016 and September 13, 2016, [redacted] upgraded PACS software on [redacted] servers without performing the configuration change management tasks (P1.2 and P1.4). For one of the servers, [redacted] did not update the baseline configuration within 30 days after upgrading the PACS software (P1.3). [redacted] completed these tasks on August 30, 2016 (12 days after upgrading) and September 13, 2016 (same day as upgrading but after the upgrade).

237. Between August 18, 2016 and September 23, 2016, [redacted] upgraded PACS software on [redacted] workstations without performing the configuration change management tasks required in P1.2 and P1.4. For [redacted] of the workstations, [redacted] did not update the baseline configuration within 30 days after upgrading the PACS software (P1.3). The earliest due date by which [redacted] should have updated its baseline documentation was September 17, 2016. [redacted] completed these tasks on June 29, 2017.

238. On October 6, 2016, [redacted] discovered this instance while performing a security controls verification prior to a device change.

239. This instance started August 18, 2016, when [redacted] upgraded the software without performing the required tasks, and ended on October 7, 2016, when [redacted] updated the baseline configuration documentation for all Cyber Assets.

240. In the eighth instance, sometime before July 1, 2016, [redacted] installed software on [redacted] EACMS servers associated with High and Medium Impact BES Cyber Systems, but did not reflect it in the documented baseline configuration (P1.1).

241. On January 5, 2017, while preparing for a software upgrade on the [redacted] EACMS servers, an employee discovered this discrepancy and added the software to the documented baseline configuration.

242. This instance started July 1, 2016, when the Standard became mandatory and enforceable on [redacted], and ended January 5, 2017, when [redacted] updated the baseline.

243. In the ninth instance, on April 20, 2016, [redacted] commissioned [redacted] PACS controller panels at a PSP, but did not add them to the PACS asset list. As a result, the [redacted] PACS controller panels were missing documented baseline configurations on July 1, 2016, when the standard became mandatory and enforceable (P1.1).

244. In addition, on April 21, 2016, May 9, 2016, and November 22, 2016, [redacted] upgraded firmware on [redacted] PACS controller panels, each at a different PSP, but did not add them to their respective documented baseline configurations (P1.2).

245. On February 27, 2017, [redacted] discovered these discrepancies while preparing for the annual Bulk Electric System (BES) Cyber System (BCS) review.

246. On March 9, 2017, [redacted] created and updated baseline configurations for the [redacted] PACS controller panels 221 days late (P1.3).

247. This instance started on July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended March 9, 2017, when [redacted] updated the baselines.

248. In the tenth instance, since July 1, 2016, [redacted] omitted [redacted] accessible logical network ports, which were needed on [redacted] workstations, from the documented baseline configuration (P1.1).

249. On June 9, 2017, while conducting a baseline documentation review as part of mitigation activities associated with the first expansion of scope dated May 18, 2017, an employee performed a port scan of [redacted] PACS PSP monitoring workstations and discovered the ports missing from the baseline documentation.

250. This instance started July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended June 21, 2017, when [redacted] updated the baseline configurations to include the ports for the [redacted] workstations.

251. In the eleventh instance, since July 1, 2016, [redacted] installed software on [redacted] PACS monitoring workstations, but did not include it on the documented baseline configuration (P1.1).

252. On June 9, 2017, while conducting a baseline documentation review as part of mitigation activities associated with the first expansion of scope dated May 18, 2017, an employee discovered this instance.

253. This instance started July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended June 22, 2017, when [redacted] updated the baseline configuration to include the software installation for the [redacted] workstations.

254. In the twelfth instance, on April 22, 2017, [redacted] upgraded software on [redacted] PACS PSP monitoring workstations, but did not update the documented baseline configuration within 30 calendar days of completing the change (P1.3).

255. On June 9, 2017, while conducting a baseline documentation review as part of mitigation activities associated with the first expansion of scope dated May 18, 2016, an employee discovered this instance.

256. This instance started on May 22, 2017, 30 days after [redacted] upgraded the software, and ended June 22, 2017, when [redacted] updated the baseline configuration to include the software upgrade.

257. In the thirteenth instance, on May 18, 2017, [redacted] erroneously installed software on [redacted] PACS workstations without following CIP-010-2 R1 change management procedures (P1.2, P1.3, and P1.4) because the installation was unintended due to an employee oversight.

258. On June 14, 2017, while conducting a baseline documentation review as part of mitigation activities associated with the first expansion of scope dated May 18, 2016, an employee discovered this error.

259. This instance started on May 18, 2017, when [redacted] erroneously installed the software, and ended on June 15, 2017, when [redacted] uninstalled the software following required change management procedures.

260. In the fourteenth instance, on February 22, 2017 and on February 24, 2017, [redacted] erroneously installed software on [redacted] PACS workstations without following CIP-010-2 R1 change management procedures (P1.2, P1.3, and P1.4) because the installations were unintended due to an employee oversight. On June 20, 2017, an employee discovered this error while mitigating prior discoveries. On June 22, 2017, [redacted] uninstalled the software following required change management procedures.

261. This instance started on February 22, 2017, when [redacted] first erroneously installed software, and ended June 22, 2017, when [redacted] last uninstalled the software.

262. In the fifteenth instance, on April 18, 2017, [redacted] installed software on [redacted] EACMS servers associated with Medium Impact transmission substation BCS used for logging and alerting of security events, but did not update the documented baseline configuration within 30 calendar days of completing the change (P1.3).

263. On June 14, 2017, while conducting a baseline documentation review as part of mitigation activities associated with the first expansion of scope dated May 18, 2017, an employee discovered this instance.

264. This instance started on May 18, 2017, 30 days after [redacted] uninstalled the software, and ended June 14, 2017, when [redacted] updated the baseline configuration to include the software upgrade.

265. The root cause of this violation was inadequate internal controls and training due to management oversight in planning, preparing, and implementing the change management requirements associated with the transition to CIP Version 5.

266. SERC determined this violation posed a serious risk to the reliability of the BPS.[23] By [redacted] not properly documenting baseline configurations and not managing change control processes fully, there existed a degradation in situational awareness of ports in use that could lead to exploitation and malicious actors gaining control of cyber assets and BPS facilities. There are a large number of instances associated with this violation. However, none of the issues directly impacted BES Cyber Systems or their associated Protected Cyber Assets, but only impacted associated cyber assets or systems that supported the BES Cyber Assets. The Cyber Assets involved utilized two-factor authentication access controls and [redacted] physically secured them within PSPs. Except for the two instances of unintentional installation of software, all ports, patches, software, and firmware upgrades were applicable and required. Therefore, this violation mostly involved documentation issues related to baseline configurations. [redacted] found no exploitation and no CIP-005 nor CIP-007 noncompliance due to the baseline configuration misses. In addition, a newly formed CIP team within [redacted] was responsible for the errors noted in this violation. The new team was created to help manage access control for a small portion of Cyber Assets at Medium Impact substations under CIP Version 5. For the second instance, while [redacted] documented an overly broad range of open ports, it did not open or use any unnecessary ports due to the exterior firewall rules preventing access and use of these ports. [redacted]

[23] According to the CIP-010-2 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Lower" VSL.

Attachment A

Mitigating Actions for SERC2016016321

267. On February 8, 2019, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-010-2 R1, Part 1.1, including all instances identified in the Self-Reports and the subsequent expansion of scope. *See* Mitigation Plan for SERC2016016321. On March 5, 2019, SERC accepted the Mitigation Plan.

268. To mitigate this violation, [redacted]

i. updated the entity's baseline documentation to include the open port involved in the first instance;
ii. reviewed the entity's baseline documentation to ensure all authorized logical network accessible ports are included;
iii. implemented a secondary supervisor review of any changes to the transmission baseline documentation and business justifications to ensure all ports enabled and required for operations are included in the associated baseline documentation. Supervisory review shall be captured in the baseline change log;
iv. updated its baseline documentation to include the missing open and required port;
v. performed a review of all CIP cyber system baseline documentation, and verified all are up to date and accurate, and included any installs, upgrades, or updates implemented prior to July 1, 2016;
vi. conducted a review session of the applicable entity IT work practices addressing CIP-010-2 R1.1 and retrained department personnel on updating baseline documentation within the required timeframes;
vii. required departmental personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps and agree to abide by the procedures going forward;
viii. consolidated and moved all EACMS servers to a common domain in order to facilitate a more controlled deployment of approved changes and ensure baseline updates occur in a timely fashion;
ix. updated baseline documentation to reflect the version upgrade to the agents for the [redacted]EACMS servers;
x. excluded all CIP PACS systems from "roll-up" patch deployment collections and moved them to collections for all future targeted CIP security patch deployments;
xi. updated the PACS baseline documentation to include the missing software upgrade;
xii. updated the PACS baseline documentation to include the PACS controller panel firmware upgrades and PACS controller replacements;

Attachment A

xiii. conducted a review and oversight session with executives over the entity's technology organization to emphasize the importance of compliance with the CIP Standards;

xiv. reviewed the entity's IT work Practices applicable to CIP-010-2 R1 for areas where additional instruction was added to help prevent re-occurrences;

xv. implemented organizational changes to the [redacted] structure to provide additional personnel responsible for CIP compliance tasks to prevent future issues of the same or similar requirements;

xvi. reviewed each configuration management tool to ensure CIP assets were not included into any enterprise rollup groups to prevent unintentional deployment of updates outside the CIP change management process where possible;

xvii. performed a review of all domains and PACS baseline documentation, and verified all are up to date and accurate;

xviii. conducted a review and training session with departmental personnel and management on applicable changes to the entity's IT work practices addressing CIP-010-2 R1;

xix. conducted a review and retraining session with PACS system administrators on the process for replacing controller panel hardware;

xx. completed a comprehensive review of all required evidence associated with this mitigation plan and prepared and submitted a closure packet for SERC review of these potential violations;

xxi. implemented technical controls to perform a line by line comparison between the baseline documentation software inventory and the software actually installed on the systems;

xxii. developed and deployed technical controls to perform a comparison between the baseline configuration ports and services whitelist and the listening ports and services derived from the output of the protocol and ports identification tool;

xxiii. updated the PACS ports and services whitelist as part of the baseline documentation to include the necessary ports that were missed;

xxiv. updated the PACS workstations inventory as part of the baseline documentation to include the upgraded missing applications;

xxv. verified the erroneously installed software was removed from the PACS Workstations; and

xxvi. implemented changes to the configuration management tool, to limit the number of administrators with the ability to update CIP Assets.

269. On February 8, 2019, [redacted] certified to SERC that it completed the Mitigation Plan as of July 18, 2017. *See* Certification of Mitigation Plan Completion for SERC2016016321.

Attachment A

Description of Alleged Violation and Risk Assessment for SERC2018019106

270. On October 30, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-010-2 R1, Part 1.4. *See* Self-Report for SERC2018019106. [redacted] had [redacted] instances where it did not implement a documented process that includes, for a change that deviates from the existing baseline configuration, prior to the change, determining required security controls in CIP-005 and CIP-007 that could be impacted by the change (P1.4.1), following the change, verify that required security controls are not adversely affected (P1.4.2), and documenting the results of the verification (P1.4.3).

271. On November 18, 2016, [redacted] completed a firmware update which caused resetting of passwords back to the factory default passwords for the administrator accounts of [redacted] BES Cyber Systems. Additionally, on December 16, 2016, during a firmware update, [redacted] reset passwords to factory default on [redacted] BCSs at a second substation. These [redacted] BCSs were the same model of devices as the other [redacted]

272. On October 9, 2017, an [redacted] field employee discovered the first [redacted] deficient passwords while performing routine Cyber Asset maintenance at a substation. On October 11, 2017, [redacted] discovered the additional [redacted] deficient passwords while it conducted a [redacted] extent-of-condition assessment. [redacted] found no additional issues at the remaining [redacted] operating companies.

273. [redacted]

274. The root cause of this violation was insufficient field procedures, as well as associated functional testing, training and oversight-related situational awareness covering their application.

275. This violation started on November 18, 2016, the earliest instance where [redacted] changed passwords to default during firmware updates, and ended on October 12, 2017, when [redacted] changed the [redacted] passwords to CIP-compliant passwords.

276. SERC determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[24] By resetting passwords to factory default, there was an increased potential for the intrusion and exploitation of BCS, in that malicious actors could gain operational control of BPS facilities and maliciously cause grid instability. However, [redacted] did not enable IRA and [redacted] protected all affected BCSs within PSPs and ESPs. [redacted] had continuous electronic monitoring of PSPs. For [redacted] of [redacted] instances, [redacted] had continuous electronic monitoring in place. For the remaining [redacted] instances, [redacted] had a maximum lag time in electronic detection of 24 hours. [redacted] had continuous monitoring of a non-

[24] According to the CIP-010-2 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

CIP nature in place that would have alerted systems operations personnel immediately of any setting changes that caused communication channel failure.

Mitigating Actions for SERC2018019106

277. On February 2, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-010-2 R1, Part 1.4. *See* Mitigation Plan for SERC2018019106. On February 19, 2019, SERC accepted the Mitigation Plan.

278. To mitigate this violation, [redacted]

i. changed the local default administration account passwords on the involved devices;
ii. conducted a review and training session with [redacted] and affiliate operating company personnel on the CIP-010-2 baseline configuration change management work practice; and
iii. added additional instruction to the CIP-010-2 baseline configuration change management work practice as an additional guide for testing CIP-005 and CIP-007 security controls.

279. On April 27, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of April 27, 2018. *See* Certification of Mitigation Plan Completion for SERC2018019106.

M. CIP-011-2 R1 (SERC2016016379, SERC2016016572, and SERC2017017564)

280. CIP-011-2 helps prevent 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).

281. CIP-011-2 R1 states in relevant part:

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection.

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.

Description of Alleged Violation and Risk Assessment for SERC2016016379

282. [redacted] SERC sent [redacted] an ADL notifying it of a Compliance Audit scheduled for [redacted] with the on-site week being the week of [redacted]

283. On [redacted], [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-011-2 R1, Part 1.2. *See* Self-Report for [redacted] failed to protect and securely handle BES Cyber System Information (BCSI) in accordance with its information protection program.

284. Prior to July 1, 2016, [redacted] stored a file containing BCSI on a corporate network shared drive, which was not identified in [redacted] information protection program as a BCSI repository. Since [redacted] did not specify the location pursuant to the BCSI information protection program, [redacted] did not implement secure handling and storage of BCSI in conformance with the documented program. The improperly stored BCSI impacted the Cyber Assets and their associated Electronic Access Control or Monitoring System (EACMS) and Physical Access Control System (PACS) for all [redacted] substations containing medium impact BES Cyber Systems (BCSs). [redacted]

285. On July 20, 2016, a [redacted] manager discovered this noncompliance while performing a review of employees' access.

286. [redacted] conducted an extent-of-condition assessment by reviewing all repositories managed by the new compliance team involved in the instant noncompliance that had responsibility for CIP Compliance in substations and specifically EACMS and PACS (a limited number of sites and applications). [redacted] did not find any additional instances of noncompliance.

287. The root cause of this violation was oversights in procedures and training associated with the transition to CIP-011-2 (CIP Version 5).

288. This violation started on July 1, 2016, when the standard became mandatory and enforceable on [redacted] and ended on July 29, 2016, when [redacted] moved the BCSI to a BCSI repository.

289. This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS.[25] By not storing BCSI in a designated repository, there was an enhanced potential for inadequate access controls that could allow malicious actors to access and utilize the information to gain operational control of cyber assets and BPS facilities and cause harm to grid security. However, [redacted] was aware of the sensitivity of the BCSI and stored it securely in a manner that controlled membership and prohibited outside access. [redacted] controlled access

[25] According to the CIP-011-2 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

to the non-BCSI location at the domain level, with access granted only to qualified personnel on the basis of business need. In addition, [redacted] afforded protection of the BCSI at the file level by employing password secured encryption.

Mitigating Actions for SERC2016016379

290. On October 19, 2016, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-011-2 R1, Part 1.2. *See* Mitigation Plan for SERC2016016379. On February 18, 2019, SERC accepted the Mitigation Plan.

291. To mitigate this violation, [redacted]

i. moved the involved file to a BCSI repository;
ii. changed the password to access the involved file and provided it verbally to those resources with authorized access;
iii. performed a review to verify there are no additional instances of BCSI that [redacted] IT owns or manages that is not properly stored in a documented BCSI repository; and
iv. retrained department personnel and managers on the entity's CIP information protection program.

292. On December 8, 2016, [redacted] certified to SERC that it completed the Mitigation Plan as of November 30, 2016. *See* Certification of Mitigation Plan Completion for SERC2016016379.

Description of Alleged Violation and Risk Assessment for SERC2016016572

293. On November 28, 2016, [redacted] submitted a Self-Report to SERC stating that, as a [redacted] it was in violation of CIP-011-2 R1, Part 1.2. *See* Self-Report for SERC2016016572. Subsequently, on March 14, 2017, [redacted] submitted an expansion of scope with additional instances of noncompliance with CIP-011-2 R1, Part 1.2. This violation involves six instances where [redacted] failed to protect and securely handle BCSI.

294. Sometime prior to July 1, 2016, [redacted] printed [redacted] substation drawings containing BCSI and appropriately marked them to indicate BCSI. Later, when [redacted] updated the electronic versions to remove the BCSI data, it did not print new hard copies. Further, [redacted] did not destroy the old versions and did not maintain the old versions within a designated BCSI repository. [redacted] did not securely handle the physical drawings in a controlled access repository in conformance with the documented information protection program.

295. On September 14, 2016, an [redacted] manager discovered the first three instances during the course of normal work activities.

296. On September 15, 2016, [redacted] completed an extent-of-condition assessment for the first three instances by inspecting all relevant [redacted] office areas for physical copies

of drawings. [redacted] identified no additional similar instances. In addition, [redacted] confirmed that [redacted] and [redacted] had destroyed all physical copies of drawings containing BCSI prior to July 1, 2016.

297. On September 9, 2016, [redacted] employees stored two files containing BSCI on a shared corporate network drive not designated as a BCSI repository and transmitted one unencrypted file containing BCSI via email to [redacted] employees. Since the documented information protection program did not identify the shared corporate network drive as a BCSI repository, and since the program did not permit unencrypted transmissions of BCSI as an acceptable means of transit, [redacted] did not protect and securely handle the information including storage and transit according to the documented program.

298. On September 28, 2016, [redacted] discovered the additional three instances during SERC's extent-of-condition assessment to determine the scope of the violation.

299. On September 29, 2016, [redacted] removed the BCSI from the two files stored on the shared corporate network drive and the email recipients at [redacted] deleted the email containing the unencrypted BCSI. [redacted] IT also ran a tool to find all emails with unencrypted BCSI within its email servers and deleted all instances there also.

300. [redacted] employees completed an extent-of-condition assessment for the second three instances by conducting an internal investigation with employees at each [redacted] operating company with the ability to view or access the type of BCSI involved in the breach. The employees found no additional instances of improper storage or transmission.

301. [redacted]

302. The root cause of this violation was insufficient training and internal controls regarding transitioning to CIP-011-2.

303. This violation started on July 1, 2016, when the CIP Version 5 Standard became mandatory and enforceable on [redacted] and ended on September 29, 2016, when [redacted] removed the BCSI from the two files stored on the shared corporate network drive and the email recipients at [redacted] deleted the email.

304. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS.[26] By not securely handling and storing BCSI, there was a potential for malicious actors to gain an understanding of network configurations or other sensitive data to gain operational control of Cyber Assets

[26] According to the CIP-011-2 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

and BPS Facilities. However, in the first three instances, [redacted] physically protected the drawings on company premises and controlled access to them using badge readers. In the second three instances, [redacted] secured access to the corporate network with passwords and the recipients of the email had CIP personnel risk assessments and cyber security training. For all instances, [redacted] protected affected Cyber Assets with access controls such that malicious actors could not have gained control of them. In addition, [redacted] protected the Cyber Assets by way of additional defense-in-depth provisions, including securing them behind a firewall in an ESP and enclosing them within PSPs.

Mitigating Actions for SERC2016016572

305. On November 28, 2016, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-011-2 R1, Part 1.2, including all instances identified in the Self-Report and the subsequent expansion of scope. *See* Mitigation Plan for SERC2016016572. On March 7, 2019, SERC accepted the Mitigation Plan.

306. To mitigate this violation, [redacted]

i. reviewed involved office areas to locate all hardcopy files with BCSI to confirm all printed files are stored correctly or have been shredded;
ii. destroyed all documents with BCSI that were stored incorrectly; and
iii. retrained involved employees on the entity's NERC CIP information protection procedure.

307. On March 1, 2019, [redacted] certified to SERC that it completed the Mitigation Plan as of May 12, 2017. *See* Certification of Mitigation Plan Completion for SERC2016016572.

Description of Alleged Violation and Risk Assessment for SERC2017017564

308. On May 15, 2017, [redacted] submitted a Self-Report to SERC stating that, as a [redacted], it was in violation of CIP-011-2 R1, Part 1.2. *See* Self-Report for SERC2017017564. [redacted] failed to protect and securely handle BCSI.

309. In approximately [redacted] instances, [redacted] employees stored and transmitted shared account passwords to BCSs in a manner that did not conform to [redacted] documented information protection program. [redacted] classified this information as BCSI in the information protection program. Specifically, [redacted] employees stored approximately [redacted] BCSI relay test sheets on corporate network drives. Of the approximate [redacted] test sheets, [redacted] employees stored about [redacted] in restricted SharePoint folders or restricted network drives and stored about [redacted] on less restricted individual employee network drives. Further, [redacted] employees transmitted about [redacted] of these test sheets unencrypted via email to other [redacted] relay

technicians. A total of [redacted] employees in [redacted] business units responsible for Protection System maintenance were involved in these instances.

310. [redacted] could not definitively determine the scope of affected [redacted] facilities and Cyber Assets, since it did not create any records of saving documentation outside of the BCSI repository.

311. Between January 23, 2017 and February 3, 2017, in the course of conducting an extent-of-condition assessment associated with a related [redacted] violation (NERC Violation ID: SERC2016016572), [redacted] discovered these instances of noncompliance [redacted] shared its discovery with the [redacted]. All [redacted] operating companies assessed the condition and found no additional instances of the same problems occurring elsewhere.

312. SERC determined the root cause of this violation was insufficient training.

313. This violation started on July 1, 2016, when the Standard became mandatory and enforceable on [redacted] and ended on August 13, 2018, when [redacted] deleted the passwords from the shared drive locations and deleted all instances of the emails.

314. This violation posed a moderate risk to the reliability of the BPS.[27] By [redacted] not securely storing and transmitting BCSI, there was a potential for malicious actors to intercept sensitive information and gain access to BES Cyber Systems, operate BES Facilities, and cause grid instability. However, [redacted] stored the BCSI on corporate networks and local drives that required access credentials. [redacted] protected the affected BCSs behind firewalls within ESPs inside PSPs. [redacted] also had electronic monitoring of network traffic and physical access to BCSs in place at all times to alert personnel of malicious intrusion. Although [redacted] had provisioning in place which allowed interactive remote access to BCSs, two-factor authentication was required.

Mitigating Actions for SERC2017017564

315. On September 4, 2018, [redacted] submitted a Mitigation Plan to SERC, addressing the Alleged Violation of CIP-011-2 R1, Part 1.2. *See* Mitigation Plan for SERC2017017564. On February 18, 2019, SERC accepted the Mitigation Plan.

316. To mitigate this violation, [redacted]

i. required managers to review all individuals with view passwords role in compliance management tool to determine if the scope of individuals with this role can be reduced to further restrict access to passwords where needed;

[27] According to the CIP-011-2 Table of Compliance Elements, this noncompliance warrants a "Medium" VRF and a "Severe" VSL.

ii. drafted a substation field guide specifically addressing the proper protection and secure handling of BCSI, including storage, transit, and use, where applicable, and new request processes and secure storage of passwords; and

iii. conducted retraining of all personnel with view passwords role in compliance management tool on the configuration changes in compliance management tool to prevent the inadvertent downloading of device passwords in the future, and train personnel on Substation procedures on protecting and securely handling BCSI, including storage, transit, and use.

317. On September 4, 2018, [redacted] certified to SERC that it completed the Mitigation Plan as of May 19, 2017. *See* Certification of Mitigation Plan Completion for SERC2017017564.

Attachment 2

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

2a. The Entities' Self-Report (SERC2016015954)

2b. The Entities' Mitigation Plan designated as SERCMIT014422 submitted February 8, 2019.

2c. The Entities' Certification of Mitigation Plan Completion submitted April 19, 2019.

VIEW SELF-REPORT: CIP-002-5.1 R1. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 7/25/2016

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]
Applicable Requirement:	[redacted]
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:	7/1/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	10/1/2017
Is the violation still occurring?	Yes

Provide detailed description and cause of Possible Violation:

While reviewing the list of substation facilities to determine which substations contain Low Impact BES Cyber Systems in preparation for CIP Version 5, it was discovered that [redacted] has Transmission devices (Low-Impact BES Cyber Assets) in BES substations[redacted]oss the stat[redacted]ntrolled by DSCADA rather than the Energy Management System ("EMS"). Since January 2016, [redacted] has been in the process of implementing additional communications paths in order to poll and control those transmission devices directly from the EMS, and take the DSCADA systems out of scope. As of July 1, 2016, [redacted] had [redacted] BES substations where mitigation conversion is in progress.

Are Mitigating Activities in progress or completed? Yes

If Yes, Provide description of Mitiga ing Activities:

On January 10, 2016, [redacted] and [redacted] representatives met with SERC to discuss the situation and seek guidance on how best to move forward. [redacted] has developed a prioritized conversion plan of the Substations to transition control from DSCADA to EMS. A project schedule with progress reporting dates will be provided to SERC as an attachment to the mitigation plan associated with this self-report. [redacted] Operations Compliance, as an agent for [redacted], will submit progress reports every 90 days to SERC in accordance with the mitigation plan associated with this self-report showing the progress of the supplied conversion plan. Any opportunity to complete this conversion project ahead of schedule will be reported to SERC.

Provide details to prevent recurrence:

Successful completion[redacted]he ab[redacted]stated mitigation plan and conversion of the DSCADA control to the EMS will eliminate this issue. [redacted]

[redacted] [redacted]

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

10/1/2017

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. [redacted] currently has both physical and electronic protections in place that include the following:
1. Physical protections –
a. The data centers containing the DSCADA Cyber Assets have biometric and proximity card readers implemented to restrict physical access to authorized personnel.
b. [redacted] of the [redacted] data centers containing the DSCADA Cyber Assets are within existing CIP PSPs.
c. All Control Centers have access controlled by physical barriers and biometric and proximity card access controls that comply with CIP-006-6 R1.3.

2. Electronic protections –
a. The network is segmented into zones with DSCADA located in the most protected production zone on separate VPNs protected by firewalls.
b. No direct Internet access or corporate network [redacted] access is allowed in or out of the production zone.
c. System logging and event correlation is performed by [redacted] appliances monitoring all network connected assets.
d. All logged data and correlated events are monitored locally by DSCADA administrators and Security Operations Center (SOC) personnel 24/7.
e. IPS equipment is installed at all physical locations of the DSCADA Cyber Assets.
f. User access to the DSCADA application is role based and authorized through an access management application ([redacted]).
g. Antivirus and Malware prevention tools are used and updated on all Windows based systems.
h. Windows servers and workstations are patched and updated by centralized administrative personnel.
i. Application and operating system software updates and patches are tested on separate QC test systems before being deployed into the production environment.
j. Windows servers and workstations are periodically scanned for vulnerabilities and mitigated.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. A thorough review of the assets containing Low Impact BES [redacted]ADA determined that the primary communication path at these substations was [redacted] radio, and [redacted] radio is currently only controllable via DSCADA. Current transmission controls and data are sent fr[redacted] SCADA to EMS, and vice versa, using Inter-Control Center Communications Protocol (ICCP). Given he above listed physical and electronic protections of these systems, actual risk is considered minimal during in[redacted]menta[redacted]n of additional communications paths in order to control these Low Impact BES Cyber Assets directly from the EMS.

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)

Potential Impact to the Bulk Power System: Minimal

Actual Impact to the Bulk Power System: Minimal

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Potential Risk to Bulk Power System:

This issue poses a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. [redacted] currently has both physical and electronic protections in place that include the following:
1. Physical protections –
a. The data centers containing the DSCADA Cyber Assets have biometric and proximity card readers implemented to restrict physical access to authorized personnel.
b. [redacted] of the [redacted] data centers containing the DSCADA Cyber Assets are within existing CIP PSPs.
c. All Control Centers have access controlled by physical barriers and biometric and proximity card access controls that comply with CIP-006-6 R1.3.

2. Electronic protections –
a. The network is segmented into zones with DSCADA located in the most protected production zone on separate VPNs protected by firewalls.
b. No direct Internet access or corporate network [redacted] access is allowed in or out of the production zone.
c. System logging and event correlation is performed by [redacted] appliances monitoring all network connected assets.
d. All logged data and correlated events are monitored locally by DSCADA administrators and Security Operations Center (SOC) personnel 24/7.
e. IPS equipment is installed at all physical locations of the DSCADA Cyber Assets.
f. User access to the DSCADA application is role based and authorized through an access management application ([redacted]).
g. Antivirus and Malware prevention tools are used and updated on all Windows based systems.
h. Windows servers and workstations are patched and updated by centralized administrative personnel.
i. Application and operating system software updates and patches are tested on separate QC test systems before being deployed into the production environment.
j. Windows servers and workstations are periodically scanned for vulnerabilities and mitigated.

Provide detailed description of Actual Risk to Bulk Power System:

This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. A thorough review of the assets containing Low Impact BES [redacted]ADA determined that the primary communication path at these substations was [redacted] radio, and [redacted] radio is currently only controllable via DSCADA. Current transmission controls and data are sent fr[redacted] SCADA to EMS, and vice versa, using Inter-Control Center Communications Protocol (ICCP). Given he above listed physical and electronic protections of these systems, actual risk is considered minimal during in[redacted]menta[redacted]n of additional communications paths in order to control these Low Impact BES Cyber Assets directly from the EMS.

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)

VIEW FORMAL MITIGATION PLAN: CIP-002-5.1 (REGION REVIEWING MITIGATION PLAN)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 2/8/2019

This item was marked ready for signature by [redacted] on 2/7/2019

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-002-5.1 R1.	SERC2016015954	SERC2016-402419	08/19/2016	Revision Requested	Formal	
CIP-002-5.1 R1.	SERC2016015954	SERC2016-402419	02/08/2019	Region reviewing Mitigation Plan	Formal	1

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: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	SERC2016-402419	SERC2016015954	7/25/2016

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

While evaluating the list of substation BES Facilities prior to the effective date of CIP Version 5 to determine which substations contain Low Impact BES Cyber Systems as per CIP-002-5.1 R1, it was discovered that [redacted] has Transmission devices (Low-Impact BES Cyber Assets) in BES substations across the state controlled by DSCADA rather than the Energy Management System ("EMS"). Since January 2016, [redacted] has been in the process of implementing additional communications paths in order to poll and control those transmission devices directly from the EMS, and take the DSCADA systems out of scope. As of July 1, 2016, [redacted] had [redacted] remaining BES substations where mitigation conversion of these communication paths remained in progress.

The root-cause of this issue was that while executing its CIP-002-5 evaluations of BES Facilities and identification of medium and low-impact BES Cyber Assets/Systems prior to the effective date of CIP Version 5, [redacted] determined that there were low-impact BES Cyber System transmission devices located in BES substations whose primary communication path for control purposes was through the DSCADA (Distribution Supervisory Control and Data Acquisition) system. It was assessed at the time that this capability would bring the [redacted] DSCADA system into scope as a medium-impact BES Cyber System as of 7/1/2016 based on its usage by the [redacted] Transmission Control Center to control low-impact BES Cyber Assets/Systems at two or more low-impact BES Substation Facilities. [redacted] made the business decision in 2015 to embark on a project to implement additional communication paths in order to poll and control those transmission devices directly from the EMS and take the DSCADA system out of scope. Based on the large number of BES Facilities and communications paths needing remediation, [redacted] was unable to convert all of the identified substa ions control from DSCADA to EMS by the CIP version 5 effective date of July 1, 2016.

Attachments ()

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

On January 10, 2016, [redacted] and [redacted] representatives met with SERC to discuss the situation and [redacted]k guidance on how best to move forward. [redacted] has developed a prioritized conversion plan of the Substations to transition control from DSCADA to EMS. A project schedule with progress reporting dates will be provided to SERC as an attachment to this mitigation plan. [redacted], will submit progress reports every 90 days to SERC in accordance with this mitigation

plan showing the progress of the supplied conversion plan. Any opportunity to complete this conversion project ahead of schedule will be reported to SERC.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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:

[redacted] has developed a conversion plan that removed the DSCADA controls from all [redacted] substations containing Low Impact BES Cyber Systems by implementing additional communication paths, and adjusted the Remote Terminal Units (RTUs) and EMS databases to poll the transmission devices directly from the EMS. The conversion plan was completed on October 1, 2017.

The conversion plan included a breakdown of the [redacted] substations into groups where mitigation was completed for each group in accordance with the conversion plan schedule.

1. [redacted] DSCADA Conversion Plan Progress Report (Due: 10/15/2016 and Completed 10/14/2016)
[redacted] has developed a conversion project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 10/14/2016 - [redacted] completed mitigation at [redacted] of the [redacted] BES Substa ion Facilities.

2. [redacted] DSCADA Conversion Plan Progress Report
Milestone Completed (Due: 1/15/2017 and Completed 1/5/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 1/5/2017 - [redacted] completed mitigation at [redacted] of the [redacted] BES Substation Facilities.

3. [redacted] DSCADA Conversion Plan Progress Report
Milestone Completed (Due: 4/15/2017 and Completed 3/29/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 3/29/2017 - [redacted] completed mitigation at [redacted] of the [redacted] BES Substation Facilities.

4. [redacted] DSCADA Conversion Plan Progress Report
Milestone Completed (Due: 7/15/2017 and Completed 7/14/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 7/14/2017 - [redacted] completed mitigation at [redacted] of the [redacted] BES Substation Facilities. Between 7/1/2016 and 4/15/2017, [redacted] Transmission has been ahead of schedule on this conversion project as outlined in the original self-report for this issue; however, [redacted] work schedule and business needs during this summer load period have not permitted the [redacted] and [redacted] substations to be taken out of service for conversion to EMS during the period from 4/15/2017 until 7/14/2017. The [redacted] and [redacted] substations are currently scheduled to be taken out of service during the month of August to complete the DSCADA conversion to EMS ahead of the final milestone completion date of 10/1/2017 for this mitigation plan.

5 [redacted] DSCADA Conversion Plan Completion Report
Milestone Completed (Due: 10/1/2017 and Completed 9/7/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 9/7/2017 - [redacted] completed mitigation at all of the [redacted] BES Substation Facilities.

Attachments ()

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:

10/1/2017

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

1. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 10/15/2016 and Completed 10/14/2016)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

2. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 1/15/2017 and Completed 1/5/2017)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

3. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 4/15/2017 and Completed 3/29/2017)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

4. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 7/15/2017 and Completed 7/14/2017)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

5. [redacted] DSCADA Conversion Plan Completion Report

Milestone Completed (Due: 10/1/2017 and Completed 9/7/2017)

[redacted] has developed a conversation project that would remove the DSCADA controls from al[redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing [redacted] project each 90 days.

NOTICE: THE FOLLOWING CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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):

(i) There are no additional risks or impacts to the Bulk Power System while the actions in this Mitigation Plan are being completed. This issue poses a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. A thorough review of the assets containing Low Impact BES Cyber Assets controlled by DSCADA determined that he primary communication path at these substations was [redacted], and [redacted] is currently only controllable via DSCADA. Current transmission controls and data are sent from DSCADA to EMS, and vice versa, using Inter-Control Center Communications Protocol (ICCP). Given the below listed physical and electronic protections of these systems, actual risk is considered minimal during implementation of additional communications paths in order to control these Low Impact BES Cyber Assets directly from the EMS.

(ii)[redacted] does not plan to implement additional actions that would increase risks to the reliability of the Bulk Power System as part of this Mitigation Plan. Existing security measures already in place to reduce risk during execution of this mitigation plan in the following physical and electronic security measures:
3. Physical protections –
a. [redacted]
b. [redacted] of the [redacted] data centers containing the DSCADA Cyber Assets are within existing CIP PSPs.
c. [redacted] s that comply with CIP-006-6 R1.3.
4. Electronic protections –
a. The network is segmented into zones with DSCADA located in the most protected production zone on separate VPNs protected by firewalls.
b. No direct Internet access or corporate network ([redacted] access is allowed in or out of the production zone.
c. System logging and event correlation is performed by [redacted] appliances monitoring all network connected assets.
d. All logged data and correlated events are monitored locally by DSCADA administrators and Security Operations Center (SOC) personnel 24/7.
e. IPS equipment is installed at all physical locations of the DSCADA Cyber Assets.
f. User access to the DSCADA application is role based and authorized through an access management application ([redacted]).
g. Antivirus and Malware prevention tools are used and updated on all Windows based systems.
h. Windows servers and workstations are patched and updated by centralized administrative personnel.
i. Application and operating system software updates and patches are tested on separate QC test systems before being deployed into the production environment.
j. Windows servers and workstations are periodically scanned for vulnerabilities and mitigated.

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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):

Successful completion[redacted]he ab[redacted]mitigation plan milestones will eliminate this issue and take[redacted] DSCADA out of scope for CIP compliance[redacted]rposes.

[redacted]

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 SERC 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 Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-002-5.1 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 4/19/2019

This item was marked ready for signature by [redacted] on 2/7/2019

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R1.	SERC2016-402419	SERC2016015954

Date of completion of the Mitigation Plan:

[redacted]

1. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 10/15/2016 and Completed 10/14/2016)
Attachments (0)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

2. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 1/15/2017 and Completed 1/5/2017)
Attachments (0)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

3. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 4/15/2017 and Completed 3/29/2017)
Attachments (0)

[redacted] has developed a conversation project that would remove the DSCADA controls from al [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

4. [redacted] DSCADA Conversion Plan Progress Report

Milestone Completed (Due: 7/15/2017 and Completed 7/14/2017)
Attachments (0)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

5. [redacted] DSCADA Conversion Plan Completion Report

Milestone Completed (Due: 10/1/2017 and Completed 9/7/2017)
Attachments (0)

[redacted] has developed a conversation project that would remove the DSCADA controls from all [redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days.

Summary of all actions described in Part D of the relevant mitigation plan:

[redacted] eloped a conversion plan that removed the DSCADA controls from all [redacted] substations containing Low Impact BES Cyber Systems by implementing additional communication paths, and adjusted the Remote Terminal Units (RTUs) and EMS databases to poll the transmission devices directly from the EMS. The conversion plan [redacted]

The conversion plan included a breakdown of the [redacted] ations into groups where mitigation was completed for each group in accordance with the conversion plan

schedule.

1. [redacted] DSCADA Conve[redacted]Plan Progress Report (Due: 10/15/2016 and Completed 10/14/2016)
[redacted] has developed a conversion project t[redacted]would remove the DSCADA controls from all[redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each[redacted] he[redacted] BES Substation Facilities.

NON-PUBLIC AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

2. [redacted] DSCADA Conversion Plan Progress Report
Milestone Co[redacted]ed (Due: 1/15/2017 and Completed 1/5/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all[redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Repor[redacted]sion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 1/5/[redacted]7 - [redacted] completed mitigation at[redacted] of the[redacted] BES Substation Facilities.

3. [redacted] DSCADA Conversion Plan Progress Report
Milestone Comp[redacted]
[redacted] has developed a conversion[redacted]hat would remove the DSCADA controls from all[redacted] substations containing[redacted]ct BES Cyber Systems. For each Progress Report milestone outlined below, an updated ve[redacted]n of the conversion project plan and schedule will be provided showing status towards completion of this project e[redacted]90 days. As of 3/29/2017 - [redacted] completed mitigation at[redacted] of the[redacted] BES Substation Facilities.

[redacted] DA Co[redacted]rt
Milestone Completed (Due: 7/15/2017 and Completed 7/14/2017)
[redacted] has developed a[redacted]n project that would remove the DSCADA controls from al[redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Repor[redacted]conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 7/14/2017 - [redacted] completed mitigation at[redacted] of the[redacted] BES Substation Facilities. Between 7/1/2016 and 4/15/2017, [redacted] Transmission has been ahead of schedule on this conversion project as outlined in the original self-report for this issue; however,[redacted] work schedule and business needs during this summer load period have not permitted the[redacted] and[redacted] substations to be taken out of service for conversion to EMS during the period from 4/15/2017 until 7/14/2017. The[redacted] substations are currently scheduled to be taken out of service during the month of August to complete the DSCADA conversion to EMS ahead of the final milestone completion date of 10/1/2017 for this mitigation plan.

5. [redacted] DSCADA Conversion Plan Completion Report
Milestone Completed (Due: 10/1/2017 and Completed 9/7/2017)
[redacted] has developed a conversion project that would remove the DSCADA controls from all[redacted] substations containing Low-Impact BES Cyber Systems. For each Progress Report milestone outlined below, an updated version of the conversion project plan and schedule will be provided showing status towards completion of this project each 90 days. As of 9/7/2017 - [redacted] completed mitigation at all of the[redacted] BES Substation Facilities.

Description of the information provided to SERC for their evaluation *

[redacted] DSCADA – Closure Summary
Milestone 1:
CIP-002-5.1 R1[redacted] shows the Distribu ion Supervisory Control and Data Acquisition (DSCADA) conversion process to Energy Management Systems (EMS) and the number of[redacted] BES locations to be converted from DSCADA to EMS control. The "sites complete" tab demonstrates that the sample[redacted] site control conversion was completed on 10/4/2016. The remaining sites are listed in the "sites to be completed" tab.
CIP-002-5.1 R1[redacted] The Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion process to [redacted] for the sampled[redacted] facility. The highlighted information on the Header tab shows the location[redacted] and file type (EMS). The highlighted information on [redacted]Control tab identifies BES control poin[redacted] that will be separated from DSCADA contro[redacted]he EMS Screenshot tab demonstrates that he BES control point[redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1[redacted]2, t[redacted]email on 10/5/2016 demonstrates a communica ion from the[redacted] [redacted] to the[redacted] database group confirming that the BES controls at the[redacted] facility were converte[redacted]) from DS[redacted]DA to EMS on 10/4/2016. Page 3, the email on 10/6/2016 demonstrates a communication from the[redacted] database group to the[redacted] confirming that the identified points at the[redacted] facility were removed from DSCADA.
[redacted]stone 2:
CIP-002-5.1 R1[redacted] shows the Distribu ion Supervisory Control and Data Acquisition (DSCADA) conversion process to EMS and the number of[redacted] BE[redacted]cations to be converted f[redacted]n DSC[redacted]DA to EMS control. The "sites complete" tab demonstrates that the sampled[redacted] site control conversion was completed on 11/29/2016 and the sampled[redacted] site control conversion was completed on 12/2/2016. The remaining sit[redacted]e listed in the "sites to be completed" tab.
CIP-002-5.1 R1[redacted] The Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion [redacted]ess to EMS for the sampled[redacted] facility. The highlighted information on the Head[redacted] tab shows the location[redacted]) and file type (EMS). The highlighted information on the Control tab identifies BES control poin[redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control point[redacted] communication path is now[redacted]erted to EMS from DSC[redacted]A contr[redacted].
CIP-002-5.1 R1[redacted] Page 1, the email on 12/2/2016 demonstrates a communication from the[redacted] [redacted] to the[redacted] database group confirming that the BES controls at the[redacted] facility were converted ([redacted]) from DSCADA to EMS on 11/29/2016. Page 3, the email on 12/15/2016 demonstrates a communication from the[redacted] database group to the[redacted] confirming that the [redacted]ified points at the[redacted] facility were removed from DSCADA.
CIP-002-5.1 R1[redacted] The Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion process to EMS for the sampled[redacted] facility. The highlighted information on the Header tab shows the location[redacted]) and file type (EMS). The highlighted information on the Control tab identifies[redacted] BES control points[redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control points[redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1[redacted] - the email on 12/2/2016 demonstrates a communication from the[redacted] [redacted] to the[redacted] database group confirming that the BES controls at the[redacted] facility were converted[redacted]) (completed) from DSCADA to EMS on 12/2/2016. Page 3, the email on 12/15/2016 demonstrates a communication from the[redacted] database group to the[redacted] confirming that the identified points at he[redacted] facility were removed from DSCADA.
Milestone 3:
CIP-002-5.1 R1[redacted] shows the Distribu ion Supervisory Control and Data Acquisition (DSCADA) conversion process to EMS and the number of[redacted] BES locations to be converted from DSCADA EMS control. The "sites complete" tab demonstrates that the sampled[redacted] [redacted] site conversion was completed on 3/29/2017, the sampled[redacted] site conversion was completed on 2/3/2017, and the[redacted] site conversion was completed on 3/22/2017. The remaining sites[redacted] are listed in the "sites to be completed" tab.
CIP-002-5.1 R1[redacted] Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion process to EMS for the sampled[redacted] facility. The highlighted information on the Header tab shows the location[redacted] and file type (EMS). The highlighted information on the Control tab identifies two BES control points[redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control points[redacted] communica ion path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1[redacted] the email on 6/12/2017 demonstrates a communica ion from the[redacted] [redacted] to the[redacted] database group confirming that the BES controls at the[redacted] facility were converted[redacted]) (completed) from DSCADA to EMS on 3/22/2017. Page 3, the email on 8/24/2017 demonstrates a communication from the[redacted] database group to the[redacted] confirming that the identified points at the[redacted] facility were removed from DSCADA. The reason for the time gap between control conversion and database clean up on the back end was due to the original RTU being out of service at the time.
CIP-002-5.1 R1[redacted] The Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion process to EMS for the sampled[redacted]. The highlighted information on the Header tab shows the location[redacted] and file type (EMS). The highlighted information on the Control tab identifies two BES control points[redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control points[redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1[redacted] Page 1-2, the email on 2/8/2017 demonstrates a communication from the[redacted] [redacted] to the[redacted] database group confirming that the BES controls at the[redacted] facility were converted[redacted] (completed) from DSCADA to EMS on 2/3/2017. Page 3, the email on 02/08/2017 demonstrates a communication from the[redacted] database group to the[redacted] confirming that the identified points at the[redacted] facility were removed from DSCADA.
CIP-002-5.1 R1[redacted] The Point Assignment Sheet (PA sheet) demonstrates as an example the DSCADA conversion process to EMS for the sampled[redacted]. The highlighted information on the Header tab shows the location[redacted]) and file type (EMS). The highlighted information on the Control tab identifies the BES control point[redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that

the BES control point [redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1 [redacted] the email on 3/29/2017 demonstrates a communication from the [redacted] to the [redacted] database group confirming the BES controls at the [redacted] were converted ([redacted]) (completed) from DSCADA to EMS on 3/29/2017. Page 3, the email on 03/30/2017 demonstrates a communication from the [redacted] database group to the [redacted] confirming that the identified points at the [redacted] facility were removed from DSCADA.

NONPUBLIC AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Milestone 4:
CIP-002-5.1 R1 [redacted] shows the Distribu ion Supervisory Control and Data Acquisition (DSCADA) conversion process to EMS and he number of [redacted] BES locations to be converted from DSCADA to EMS control. The "sites to be completed" tab demonstrates that there are two sites remaining [redacted] to be converted from DSCADA control to EMS control.
CIP-002-R5.1 R1 [redacted] The evidence summary provides an explanation for the reason the final two substations ([redacted]) were not converted during the period 4/15/2017 until 7/14/2017.

Milestone 5:
CIP-002-5.1 R1 [redacted] shows the Distribu ion Supervisory Control and Data Acquisition (DSCADA) conversion process to EMS and that all the [redacted] DSCADA sites have been converted to EMS control. The "sites complete" tab demonstrates the [redacted] site control conversion was completed on 7/27/2017, and the [redacted] control conversion was completed on 9/7/2017. The "sites to be completed" tab shows that there are no sites at [redacted] that need to be converted to EMS control.
CIP-002-5.1 R1 [redacted] The Point Assignment Sheet (PA sheet) demonstrates the DSCADA conversion process to EMS for the [redacted] facility. The highlighted information on the Header tab shows the location [redacted] and file type (EMS). The highlighted informa ion on the Control tab identifies two BES control points [redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control points [redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1 [redacted] Page 1-2, the email on 9/7/2017 demonstrates a communication from the [redacted] to he [redacted] database group confirming that the BES controls at the [redacted] were converted ([redacted] (completed) from DSCADA to EMS on 9/7/2017. Page 3, the email as of 8/17/2017 demonstrates a communication from the [redacted] database goup to the [redacted] confirming that the identified points at the Berry facility were removed from DSCADA. Only the BES control points at this location, noted for [redacted], were converted at this time due to construction, and is the reason for the use of the term "partially completed" in the evidence. Removal of these control points completes mitigation of this issue from a communications and control stand point.
CIP-002-5.1 R1 [redacted] The Point Assignment Sheet (PA sheet) demonstrates the DSCADA conversion process to EMS for the [redacted] facility. The highlighted information on the Header tab shows the location ([redacted] and file type (EMS). The highlighted informa ion on the Control tab identifies the BES control point [redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control point [redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1 [redacted] The Point Assignment Sheet (PA sheet) demonstrates the DSCADA conversion process to EMS for the [redacted] facility. The highlighted information on the Header tab shows the location ([redacted] and file type (EMS). The highlighted informa ion on the Control tab identifies the BES control point [redacted] that will be separated from DSCADA control. The EMS Screenshot tab demonstrates that the BES control point [redacted] communication path is now converted to EMS from DSCADA control.
CIP-002-5.1 R1 [redacted] Page 1-2, the email on 8/10/2017 demonstrates a communication from the [redacted] to the [redacted] database group confirming that the BES controls at the [redacted] were converted ([redacted]) (completed) from DSCADA to EMS on 7/27/2017. Page 3, the email on 8/17/2017 demonstrates a communication from the [redacted] database group to the [redacted] confirming that the identified points at the [redacted] were removed from DSCADA.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 3

Record documents for the violation of CIP-004-6 R5

3a. The Entities' Self-Report (SERC2017018136)

3b. The Entities' Certification of Mitigation Plan Completion submitted September 15, 2017

3c. The Entities' Self-Report (SERC2017018279)

3d. The Entities' Certification of Mitigation Plan Completion submitted September 22, 2017

VIEW SELF-REPORT: CIP-004-6 R5. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 8/7/2017

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: [redacted]

Applicable Requirement: [redacted]

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):

SERC2016016174

Date Reported to Region or Discovered by Region:

9/21/2016

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: 6/23/2017

Beginning Date of Possible Violation: 5/2/2017

End or Expected End Date of Possible Violation: 6/10/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

[redacted] Operations Compliance conducted an internal control review at the end of Q2 2017 of all employees and contractors with authorized CIP access that were terminated from [redacted] during the second quarter of 2017. The CIP access termination review identified two employees that had retired during the second quarter and did not have their individual ability for unescorted physical access or Interactive Remote Access removed within 24 hours of the effective [redacted]

The first employee retired from [redacted] effective on 5/1/2017 with over 44 years of service. The employee's last day working in the office was on 3/31/2017, he used his vacation from 4/1/2017 until his effective retirement date of 5/1/2017. The employee's manager had the employee's physical ID badge disabled in the PACS ([redacted]) system on 4/1/2017, effectively removing all of the employee's ability for unescorted physical access. However, the employee had authorized electronic access to [redacted] Transmission Substation BCS[redacted]itories; the employee's manager failed to submit the required change of employment status paperwork to [redacted] Human Resources until 5/5/2017, which resulted in access to the [redacted] BCSI repositories not being removed until 5/8/2017. Therefore, the employee had the ability to remotely access the Corporate network, and could have accessed [redacted] or [redacted] of the BCSI repositories for six days following their effective retirement date, which was longer than the timeframe required by CIP-004-6 R5.3. The [redacted] BCSI repository is used to store engineering design information, firewall requests, network topologies, and working research information on potential CIP violations. The [redacted] BCSI repository is used to store BES Cyber System and BES facility lists, vulnerability assessments, and port scans for substation and IT networks. However, the employee did not logon or access the [redacted] corporate network after 3/30/2017. During the time the employee was on vacation from 4/1/2017 until his effective retireme[redacted]of 5/1/2017, the employee's ability for unescorted physical access was removed and the employee never electronically accessed the corporate network. The employee also did not have any other electronic or Interactive Remote Access to any in-scope C[redacted]stems as of 4/1/2017.

The second employee retired from [redacted] Technology Organization effective on 6/1/2017 with over 31 years of service. The employee's last day working in

the office was on 5/4/2017, he used his vacation from 5/5/2017 until his effective retirement date of 6/1/2017. The employee's manager failed to subm[redacted]e required change of employment status paperwork to [redacted] Human Resources until 6/9/2017. The employee was authorized for unescorted physical access to [redacted] CIP PSP containing PACS and EACMS assets associated with Medium Impact BES Cyber Systems, electronic access to the Transmission Substations CIP domain ([redacted]), and electronic access to one EMS BCSI repository. At the time the employee [redacted] rminal vacation, the employee's badge. The employee did not have any Interactive Remote Access into any High or Medium Impact ESPs; however, he did have remote access to the corporate network which was not removed until 6/9/2017. The individual had the ability for physical access to a CIP PSP until his ID badge was disabled in the PACS ([redacted]) system on 6/10/2017, and he ability for electronic access to the CIP [redacted] domain and EMS BCSI repository until his network ID was disabled on 6/9/2017, which collectively was 8 days beyond the timeframe required in CIP-004-6 R5.1. However, the employee did not logon to the [redacted] corporate network or access the [redacted] domain or EMS BCSI repository after 5/31/2017, and he did not attempt to access any CIP PSPs after 5/4/2017.

NOTE: THIS CONTAINS CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Both employees retired in good standing after long and dedicated careers with [redacted] The root cause is a performance issue with two managers failing to follow the prescribed process to initiate a required change of employment status and send the paperwork to [redacted] Human Resources prior to the employee's effective date of retirement.

To prevent future recurrence, [redacted] Operations Compliance will conduct retraining with each of the managers on the issue of not following corporate processes to ensure the proper and timely termination and revocation of CIP access. Additionally, [redacted] Operations Compliance will develop specific messaging related to personnel terminations to be included in the quarterly awareness newsletter for Q3 2017.

To determine the extent of condition of this issue, the quarterly internal control of performing a review of all termination dates vs. access removal dates ensures that all instances of potential non-compliance with CIP-004-6 R5 are identified and addressed quarterly.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

[redacted] Operations Compliance conducted a review of all terminated [redacted] employees and contractors with CIP access. (Completed June 23, 2017)
The [redacted] will review PACS logs to determine if the [redacted] employee attempted to physically access any CIP areas after 6/1/2017 (Completed July 18, 2017)
[redacted] Operations Compliance will conduct a retraining with managers within the applicable business units on the Access Management Revocation Program and their responsibilities as a manager (Due September 8, 2017)
[redacted] Operations Compliance will disseminate a reinforcement message to reiterate manager's responsibilities for revoking CIP access on or before the effective date of termination. (Due September 29, 2017)
[redacted]Operations Compliance will prepare and submit a comprehensive closure packet to SERC with evidence supporting the above milestones. (Due October 6, 2017)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

10/6/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Manager Retraining	9/8/2017	[redacted] Operations Compliance will conduct a retraining with managers within the applicable business units on the Access Management Revocation Program and their responsibilities as a manager.	Yes
Reinforcement Messaging	9/29/2017	[redacted] Operations Compliance will disseminate a reinforcement message to reiterate manager's responsibilities for revoking CIP access on or before the effective date of termination.	Yes
Closure Packet	10/6/2017	[redacted]Operations Compliance will prepare and submit a comprehensive closure packet to SERC with evidence supporting the above milestones.	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 issue posed a minimal potential risk, and not a moderate or serious risk to the reliability of the Bulk Power System. The two employees were both long-term employees with over 44 and 31 years of dedicated service respectively. One employee's ability for unescorted physical access was removed at the time the employee started his vacation prior to his effective retirement date. Neither employee logged on the corporate network after their effective retirement date, which indicates neither attempted to electronically access any assets, and neither attempted to physically access any corporate facilities after their effective retirement dates.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a moderate or serious risk to the reliability of the Bulk Power System. Both employees had current personnel risk assessments on file and had completed the NERC CIP Security Training and had been properly authorized for CIP access in the company's access management application [redacted]). Both employees retired from the company after long careers and neither physically accessed a CIP area or accessed the [redacted] network after their effective date of retirement. The issue was a human performance error by two managers that failed to communicate the employee's effective retirement date to [redacted] Human Resources in a timely manner.

Additional Comments:

[redacted] [redacted]cumented and implemented Access Revocation Program which covers the processes required to support compliance with CIP-004-6 R5, as follows: [redacted]

[redacted]

Managers or their designees ar[redacted]uring that an Authorized User's ability for unescorted physical access and Interactive Remote Access to all applicable systems and assets is removed within 24 hours of their Termination by ensuring the below actions are performed:

1. [redacted] terminated user's Network ID [redacted] or any other credentials used for interactive remote authentication including, [redacted] (EMS) ID or vendor credential is disabled.
2. All access badges are disabled.

NON-PUBLIC AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Revocation and removal of unescorted physical access and Interac[redacted]mote Access to applicable systems and assets shall be initiated via the following:

1. Corporate Security – Managers shall contact the Physical Security Operations Team [redacted] to disable the terminated user's physical access badge.
2. IT Service Center – Managers or their designees shall contact the IT Service Center to disable or remove the terminated user's ability to access the Company network using their [redacted].
3. EMS Support Center – Managers or their designees shall contact the EMS Support Center to disable or remove the terminated user's ability to access the EMS network using their EMS ID.
4. Access Management Application (AMA) – Managers or their designees shall directly revoke all of the terminated user's physical and electronic CIP [redacted] access approvals in an applicable AMA.

5[redacted]esources Information System – Managers or their designees shall contact their [redacted] coordinator or the HR Direct Service Center to coordinate voluntary and involuntary Termination actions.

Managers are responsible for knowing and understanding [redacted]necessary to revoke access approvals in an applicable AMA and ensure unescorted physical access and electronic access (including Interactive Remote Access) to applicable systems and assets is removed [redacted] timeframe. Any questions related to access [redacted] and/or removal requirements or their associated processes can be directed to [redacted] Operations Compliance.

[redacted]

For a Termination action of an Authorized User, Information Owners are responsible for ensuring physical access and/or electronic access to locations used to store BES Cyber System Information is revoked and removed in accordance with Section 4.1, Access Revocation and Removal – Termination.

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)

VIEW MITIGATION PLAN CLOSURE: CIP-004-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 9/15/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R5.	SERC2017-402808	SERC2017018136

Date of completion of the Mitigation Plan:

[redacted]

Manager Retraining

Milestone Completed (Due: 9/8/2017 and Completed 9/1/2017)
Attachments (0)

[redacted] Operations Compliance will conduct a retraining with managers within the applicable business units on the [redacted] and their responsibilities as a manager.

Reinforcement Messaging

Milestone Completed (Due: 9/29/2017 and Completed 9/14/2017)
Attachments (0)

[redacted] Operations Compliance will disseminate a reinforcement message to reiterate manager's responsibilities fo[redacted]ective date of termination.

Closure Packet

Milestone Pending (Due: 10/6/2017)
Attachments (0)

[redacted] Operations Compliance will prepare and submit a comprehensive closure packet to SERC with evidence supporting the above milestones.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities: [redacted] Operations Compliance conducted a review of all terminated [redacted] employees and contractors with CIP access. (Completed June 23, 2017)
The [redacted] will review PACS logs to determine if the [redacted] employee attempted to physically access any CIP areas after 6/1/2017 (Completed July 18, 2017)
[redacted] Operations Compliance will conduct a retraining with managers within the applicable business units on the [redacted] and their responsibilities as a manager (Due September 8, 2017)
[redacted] Operations Compliance will disseminate a reinforcement message to reiterate manager's responsibilities for revoking CIP access on or before the effective date of termination. (Due September 29, 2017)
[redacted] Operations Compliance will prepare and submit a comprehensive closure packet to SERC with evidence supporting the above milestones. (Due October 6, 2017)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

[redacted] Closure Packet

Milestone 1:
[redacted] Demonstrates the review and reconciliation of employees and contractors with authorized CIP physical and electronic access that were terminated from [redacted] during the timeframe 3/27/2017 to 6/23/2017. The two employees that retired and did not have their CIP access revoked within 24 hours are identified in yellow.

Milestone 2:
[redacted] Demonstrates a review and confirmation by the [redacted] ([redacted] that the Technology Organization employee [redacted] did not use his physical ID badge to access a CIP area after 6/1/2017.

Milestone 3:
[redacted] The CIP access revocation retraining that was provided via net meetings to he individual managers in the impacted organizations.

[redacted] List of individual managers that attended the CIP access revocation retraining.

Milestone 4:

[redacted] (COMPLETED), dissemination on September 14, 2017 to all Company personnel with CIP access.

[redacted] reinforcing Manager CIP access responsibilities guidance – highlights the responsibilities of managers to revoke and remove access within the required timeframes.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIEW SELF-REPORT: CIP-004-6 R5. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 8/29/2017

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]

Applicable Requirement: [redacted]

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):

SERC2017017711

Date Reported to Region or Discovered by Region:

6/8/2017

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: 6/29/2017

Beginning Date of Possible Violation: 11/4/2016

End or Expected End Date of Possible Violation: 6/29/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On June 29, 2017, Energy Management Systems (EMS) Compliance Supervisor was informed that the electronic access to a High Impact BES Cyber Asset was not removed by the end of the next calendar day after an automated system revocation for an employee transfer. The discovery was made while performing a comparison on 06/29/2017 of the Host Processing Node ([redacted] servers composing the domain which is used as the primary production domain against the EMS Emergency Backup Site [redacted] servers composing the domain which is used as the backup domain. The [redacted] employee's transfer date was 4/5/2016, but access to the [redacted] Support Role in [redacted] was determined to be needed in their new position and was retained until 11/4/2016. Access was revoked on 11/4/2016 in the company Access Management Application [redacted] and removed the same day from the [redacted] EMS client application for accessing the [redacted] but was not removed from [redacted] on the [redacted] system until 6/29/2017.

In this case the transferred employee previously had access to several CIP entities and PSPs. As part of the transfer, the employee retained CIP access to certain areas and systems he currently had authorized electronic access and unescorted physical access to, as part of his new job duties. Later, on 11/4/2016, authorization for access was revoked in the AMA to the EMS [redacted] – [redacted] Support Role that allows a user to be granted access to the [redacted]. Access was then removed from the [redacted] assets but wasn't removed from the [redacted] assets.

The personnel responsible for administration of access to the system had mistyped the username of the transferred employee and when the results came back that the user was not on the system it appeared to him that the transferred employee was successfully removed. The issue was not caught in the quarterly reviews because the employee performing the review was operating under an incorrect assumption that removal from the primary system would automatically cause the user to be removed from the second system, as is the case for many of the clustered ancillary systems. The [redacted] and the [redacted] systems do not, in fact, share common storage for user accounts and must each be updated with user account information individually. Once this was discovered, a review of the systems was performed to verify appropriate access is provisioned.

Are Mitigating Activities in progress or completed? Yes

An informal Mitigation Plan will be created upon submittal of this Self-Report with mitigating ac ivities. If you would like to schedule a mitigation call, please contact the Region.

If Yes, Provide description of Mitiga ing Activities:

1) To assess the scope of the potential issue, EMS Compliance conducted a meeting on 6/30/2017 to assess the root cause of the issue.
2) To determine extent of condition, EMS Compliance conducted a review of access between the [redacted] and [redacted] systems to determine any other existing discrepancies. (Completed 7/30/2017)
3) EMS Compliance will conduct training with appropriate staff on provisioning and revocation applicable to [redacted] and [redacted] assets to ensure both stay in sync going forward. (Complete by 9/15/2017)
4) EMS Compliance will work with operations to develop a monthly assurance review comparing the [redacted] to [redacted] to ensure they remain in sync. (Implementation Date: 09/30/2017)
5) [redacted] will prepare a comprehensive closure packet of evidence for the above milestones to submit to SERC. (10/17/2017)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

10/17/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
EMS Retraining	9/15/2017	EMS Compliance will conduct training with appropriate staff on provisioning and revocation applicable to [redacted] and [redacted] assets to ensure both stay in sync going forward.	Yes
Monthly [redacted] Report Verification	9/30/2017	EMS Compliance will work with operations to develop a monthly assurance review comparing the [redacted] to [redacted] to ensure they remain in sync.	Yes
Closure Packet	10/17/2017	[redacted] will prepare a comprehensive closure packet of evidence for the above milestones to submit to SERC	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 issue posed a minimal potential risk and not a serious or substantial risk to the reliability of the bulk electric system. Since [redacted] is the Emergency Backup System, any changes made by the employee would have been immediately discovered by the Primary System ([redacted]. The only window of opportunity: Two failovers to the [redacted] were conducted as part of the bi-annual tests during th[redacted]me period – 12/29/2016 and 4/4/2017. The employee did not access the system during this time. Logs were reviewed and the only associated log entries found during this time were conclusively associated with the removal of the account.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk and not a moderate or serious risk to the reliability of the Bulk Power System. The emplo[redacted] had a current personnel risk assessment on file and had completed the NERC CIP Security Training. He is a long-term employ[redacted] over 22 years and was a Manager with CIP oversight[redacted] responsibilities. He only had access to the EMS[redacted] - emergency backup system. During the time where he had the ability access to the EBS, he did not access the system or interact with it in any way. Logs were reviewed and the only associated log entries found during his time were conclusively associated with the removal of the account.

Additional Comments:

[redacted] has an access revocation program [redacted] that covers the following as per CIP-004-6 R5.2:
Prior to the effective date of the Authorized User's reassignment or transfer, the outgoing and hiring managers shall coordinate and review in an applicable AMA the Authorized User's existing electronic and/or unescorted physical access approvals to the applicable systems and assets and determine if the Authorized User has a business need to retain any existing access authorization in their new role or for a transitory period. As determined by the coordinated review, the hiring manager shall complete the following actions within five (5) calendar days following the effective date of the reassignment or transfer:
a. If any of the individual's existing unescorted physical and/or electronic access to an applicable system or asset is no longer required in the new position, revoke authorization for that access in he applicable AMA.
b. If any of the individual's existing unescorted physical and/or electronic access to an applicable system or asset is temporarily required during a transitory period, certify con inued retention of that access and establish an expiration date in the applicable AMA that will revoke access authorization at the end of the transitory period.
c. If any of the individual's existing unescorted physical and/or electronic access to an applicable system or asset is required for the individual in their new position, certify continued retention of that access within the applicable AMA.
By the end of the fifth calendar day following the effective date of the reassignment or transfer, the applicable AMA shall revoke any access authorization not certified by the hiring manager as required to be retained, either long term or during a transitory 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)

VIEW MITIGATION PLAN CLOSURE: CIP-004-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 9/22/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R5.	SERC2017-402830	SERC2017018279

Date of completion of the Mitigation Plan:

[redacted]

EMS Retraining

Milestone Completed (Due: 9/15/2017 and Completed 9/6/2017)
Attachments (0)

[redacted]ill conduct training with appropriate staff on provisioning and revocation applic[redacted]to[redacted]and[redacted] assets to ensure both stay in sync going forward.

Monthly[redacted] Report Verification

Milestone Completed (Due: 9/30/2017 and Completed 9/18/2017)
Attachments (0)

[redacted]ill work with operations to develop a monthly assurance review comparing the[redacted] to[redacted] to e[redacted]e they remain in sync.

Closure Packet

Milestone Completed (Due: 10/17/2017 and Completed 9/22/2017)
Attachments (0)

[redacted] will prepare a comprehensive closure packet of evidence for the above milest[redacted] to[redacted]mit to[redacted]RC

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities: 1) To assess the scope of the potential issue, EMS Compliance conducted a meeting on 6/30/2017 to assess the root cause of the issue.
2) To determine extent of condition, EMS Compliance conducted a review of access between the[redacted] and[redacted] systems to determine any other existing discrepancies. (Completed 7/30/2017)
3) EMS Compliance will conduct training with appropriate staff on provisioning and revocation applicable to[redacted] and[redacted] assets to ensure both stay in sync going forward. (Complete by 9/15/2017)
4) EMS Compliance will work with operations to develop a monthly assurance review comparing the[redacted] to[redacted] to ensure they remain in sync. (Implementation Date: 09/30/2017)
5)[redacted] will prepare a comprehensive closure packet of evidence for the above milestones to submit to SERC. (10/17/2017)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Closure Packet:[redacted]

MS1:
[redacted] shows the role that was revoked from the AMA, but not removed from the system until 6/29/2017.
[redacted] shows the meeting on 6/30/2017 to discuss the issue, root cause and how to prevent the same issue, going forward.
[redacted] shows the[redacted] logs searching on the userid looking for any access attempts by the user. The only results that were returned represent the verification checks performed by the administrator as part of the account removal verification.
[redacted] shows the change request associated with the AMA revoke, the systems involved and a description of the removal work that was performed. The actual system removal process failed due to a mistyped userid.
MS2:
[redacted] demonstrates the findings of a verification across the systems. Everyone on the systems had appropriate AMA access granted. Several entries are highlighted in yellow and represent the users that, while they have appropriate AMA access, their IDs did not exist on all of the[redacted] /[redacted] system pairs. These missing entries were corrected on the systems.
MS3:
[redacted] shows the agenda where the issue was discussed with the administrators responsible for user management and their supervisor. They discussed why the users had to be manually removed from two sites. They also discussed the proper process for account

removal along with verification of removal.
MS4:
[redacted] demonstrates the new user verification report for paired sites. It runs monthly and notifies EMS Compliance personnel if the systems get out of sync. This allows the compliance team to follow up with the administrators and ensure that issues are addressed in a timely manner.

CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 4

Record documents for the violation of CIP-005-5 R1

4a. The Entities' Self-Report (SERC2017018774)

4b. The Entities' Certification of Mitigation Plan Completion submitted December 18, 2017

VIEW SELF-REPORT: CIP-005-5 R1. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 12/12/2017

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:	[redacted]
Applicable Requirement:	[redacted]
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:	9/13/2017
Beginning Date of Possible Violation:	9/12/2017
End or Expected End Date of Possible Violation:	9/14/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On 9/13/2017, [redacted] discovered a possible CIP-005-5 R1.1 issue in a medium impact substation when an RTU was mistakenly connected to a networking device outside the substation Electronic Security Perimeter (ESP) from 9/12/2017 until 9/14/2017.

On 9/12/2017, a [redacted] employee was performing annual routine maintenance and an authorized network configuration change to remove a device from the substation CIP ESP. During the configuration change, the employee mistakenly disconnected the RTU ethernet cable from the ESP firewall and connected the RTU ethernet cable to a router outside of the ESP. The employee thought they had unplugged and moved the ethernet cable for a separate asset that was being moved out of the ESP. The RTU in this case is classified as a Medium Impact BES Cyber Asset/System. The issue was discovered on 9/13/2017 by a [redacted] employee when the device could not be discovered during network testing related to the routine maintenance and the employee could not remotely access the RTU. On 9/14/2017, the issue was corrected when a [redacted] employee was dispatched to the substation to determine the communication issue with the RTU. The [redacted] employee discovered he errant cabling move and corrected the error. The RTU was connected outside of the ESP for approximately 48 hours.

The root cause of this issue was a failure on the part of the [redacted] employee to adequately trace the ethernet cable from the device being moved outside the ESP to the ESP firewall port. During the network change, the employee inadvertently disconnected the RTU ethernet cable, rather than the cable for the device being moved, from the ESP firewall port and connected the RTU e hernet cable to a router outside of the ESP. The physical ports on the router were active when the connection was made, however, no routable connectivity to the RTU was possible while outside of the ESP. The RTU has a static IP address configured for the ESP network that prevents communication on the [redacted] network outside the ESP. Because of the static IP address configuration, the RTU could not be reached by interactive remote access. The [redacted] is a non-Internet facing business network dedicated to transmission substations and is protected and segmented from the corporate business network for added layers of protection.

To determine the extent-of-condition, [redacted] has or will review all similar substation configuration changes and confirm all previous network configuration changes were completed as required. To mitigate this issue and prevent recurrence, [redacted] performed an investigation which involved interviewing the employees involved in the issue and identifying the root cause. Modifications to the Transmission Substations work practice containing instructions for the configuration change were made to include a verification the correct cable is removed, and adds instructions to contact [redacted] Support to verify communication with the devices is working as expected at the time of the change. In addition, training on the modifications to the work practice was completed with applicable personnel.

To demonstrate that the RTU BES Cyber Asset/System did not, and could not have established communications outside of the ESP, the following files are provided:
- CIP-005-5 R1.1 MS1 Connection Evidence
- CIP-005-5 R1.1 MS5 Network Analysis
- CIP-005-5 R1.1 MS2 [redacted] Issue Determination

Are Mitigating Activities in progress or completed?	Yes

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

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] will remove the RTU from the external substation network and reconnect the device to the CIP ESP firewall. [redacted] will provide evidence demonstrating the RTU was patched properly while it was outside the ESP. (9/14/2017)
2) [redacted] will perform an issue investigation and human performance learning event to determine and document the root cause of the issue. (9/18/2017)
3) [redacted] will update the Substation work practice based on the results of the investigation to clarify the configuration change process and add steps in the process to prevent future recurrence. (9/22/2017)
4) [redacted] will perform retraining with field services personnel on the changes to the Substations work practice to reinforce new process steps intended to prevent future recurrence. (9/26/2017)
5) [redacted] will perform a network analysis documenting the ESP and [redacted] network configuration. (11/9/2017)
6) To determine the extent of condition [redacted] will review all completed substation changes related to the implementation and confirm all BCAs are accounted for and properly secured behind ESP firewalls. (1/15/2018)
7) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review. (1/30/2018)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

1/30/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Extent of Condition	1/15/2018	6) To determine the extent of condition, [redacted] will review all completed substation changes related to the implementation and confirm all BCAs are accounted for and properly secured behind ESP firewalls.	No
Closure Package	1/30/2018	7) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	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 issue posed a minimal potential risk, and not a serious or substantial risk to the reliability of the bulk electric system. The root cause of this issue was a failure to thoroughly follow the configuration change work practice to ensure applicable changes are applied and that a routable Medium Impact BES Cyber Asset was not inadvertently connected outside the substation ESP. The employee failed to verify the correct cable was removed, accidentally removing the RTU from the ESP. The RTU is used for SCADA communications (serial), engineering access (ethernet), and event file collection (ethernet). The device was still functioning as a SCADA device, it's primary function. Only the (remote) engineering access and event file collection was affected because the ethernet connection was moved. The RTU has a static IP address configured for the ESP network that prevents communication on the [redacted] network outside the ESP. Because of the static IP address configuration, the RTU could not be reached by interactive remote access. In addition, the [redacted] network provides additional layers of protection.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. [redacted] failure to properly follow the network change configuration instructions could have allowed access to the RTU outside of a CIP ESP. However, the RTU uses a static IP and was not configured to communicate through the external substation network while connected to the [redacted] router. Any remote interactive connectivity to the RTU was not possible while the device was connected outside of the ESP. In order to access the RTU, someone would have to be physically at the device. The RTU continued communicating to its associated Control Center via a serial connection, and only the (remote) engineering access and event file collection was affected because the ethernet connection was moved. The inoperability of being able to remotely access the RTU for configuration purposes had no impact to the BES; [redacted] has several BES Cyber Assets/Systems within transmission substations that are not accessible remotely. In addition, the RTU is physically protected within a PSP, and other logical protections are in place that further minimized the actual possibility of unauthorized access.

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)

VIEW MITIGATION PLAN CLOSURE: CIP-005-5 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 12/18/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R1.	SERC2017-402923	SERC2017018774

Date of completion of the Mitigation Plan:

[redacted]

Extent of Condition

Milestone Completed (Due: 1/15/2018 and Completed 12/15/2017)
Attachments (0)

6) [redacted]etermine the extent of condition, [redacted] will review all completed substation changes related to the implementation and confirm all BCAs are accounted for and properly secured behind ESP firewalls.

Closure Package

Milestone Pending (Due: 1/30/2018)
Attachments (0)

7) [redacted] Operations Compliance will com[redacted]comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and set lement of this potential violation.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities: 1) [redacted] will remove the RTU from the external substation network and reconnect the device to the CIP ESP firewall. [redacted] will provide evidence demonstrating the RTU was patched properly while it was outside the ESP. (9/14/2017)
2) [redacted] will perform an issue investigation and human performance learning event to determine and document the root cause of the issue. (9/18/2017)
3 [redacted] will update the Substation work practice based on the results of the investigation to clarify the configuration change process and add steps in the process to prevent future recurrence. (9/22/2017)
4 [redacted] will perform retraining with field services personnel on the changes to the Substations work practice to reinforce new process steps intended to prevent future recurrence. (9/26/2017)
5) [redacted] will perform a network analysis documenting the ESP and [redacted] network configuration. (11/9/2017)
6) To determine the extent of condition, [redacted] will review all completed substation changes related to the implementation and confirm all BCAs are accounted for and properly secured behind ESP firewalls. (1/15/2018)
7) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review. (1/30/2018)

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

Milestone 1: Completed: 9/14/2017
[redacted], pages 1 -3 provides evidence showing the RTU was disconnected from the CIP ESP firewall, the while disconnected the RTU connection was in an unidentified statue due to the mismatched IP configuration. Pages 4-5, provides evidence the RTU was re-connected to the CIP ESP Firewall and connectivity was restored on 9/14/2017. Page 6 provides evidence the most recent security update was applied to the RTU.

Milestone 2: Completed: 9/18/2017
[redacted] provides the issue investigation and human performance learning event, completed 9/18/2017, where the root cause of the issue was determined and discussed with the applicable pesonnel.

Milestone 3: Completed: 9/22/2017
[redacted], provides the updated HMI re-install document based on the results of the investigation to clarify the configuration change process. In section [redacted] I" a verification was added to verify the [redacted] and [redacted] link lights. A final verification step was added instructing field personnel to contact [redacted] Support to verify the RTU and HMI are reachable via IRA. The addition of these steps will ensure the correct network cable is changed and communication to devices behind the ESP is working.

Milestone 4: Completed: 9/26/2017
[redacted], provides evidence of training with field services personnel on the changes to the Substations work practice. Pages 1-5, demonstrate on 9/19/2017, a first notification and review of the potential issue at the substation was addressed. Pages 6-9 provide the meeting notice where [redacted] reviewed the additional process steps to the HMI CIP Re-Install Document the install team.

Milestone 5: Completed: 11/8/2017

[redacted], provides the network analysis completed by [redacted] to document the ESP and [redacted] network configuration. The purpose of this document is to provide an explanation of the two distinct network configurations in the [redacted] Substation and demonstrate while the physical ports on the router were active when the connection was made, no routable connectivity to the RTU was possible while outside of the ESP.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Milestone 6: Completed 12/15/2017

[redacted] provides a spreadsheet documenting the review of the [redacted] substations where the HMI has been removed. The purpose of the review verified the confirm all BCAs are accounted for and properly secured behind ESP firewalls.

[redacted], provides sample evidence from one substation demonstrating; (1) The HMI was removed from the ESP, (2) The Port associated with the HMI is disabled, and (3) The HMI FW connectivity is removed.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 5

Record documents for the violation of CIP-005-5 R2

5a. The Entities' Self-Report (SERC2016016548)

5b. The Entities' Mitigation Plan designated as SERCMIT014395 submitted August 17, 2018

5c. The Entities' Certification of Mitigation Plan Completion submitted August 17, 2018

VIEW SELF-REPORT: CIP-005-5 R2. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 11/18/2016

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]
Applicable Requirement:	[redacted]
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:	7/15/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	7/1/2017
Is the violation still occurring?	Yes

Provide detailed description and cause of Possible Violation:

On 7/15/2016 an EMS employee discovered he was able to bypass the EMS Interactive Remote Access Intermediate System (IRA-IS) from outside the ESP when using [redacted] to access BES Cyber Assets within the ESP. CIP-005-5 R2.1 states the Responsible Entity shall: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. The EMS employee, although authorized for electronic access to all of the following assets, was able to utilize an individual non-shared user account to [redacted] from the EMS [redacted] (Test [redacted] Environment), to the EMS [redacted] (Production [redacted] Environment). Upon discovery, the employee reported the issue to EMS Security for investigation. An initial investigation revealed the EMS employee did use the EMS IRA-IS to move from his EMS Desktop to the EMS [redacted] asset, but then used [redacted] to move directly from the EMS [redacted] asset outside the ESP to the EMS [redacted] asset within he ESP, bypassing the EMS IRA-IS system.

As of July 1, 2016, as part of the IRA-IS solution implementation, [redacted] was determined to be necessary for application usage for EMS [redacted] between the Production [redacted] environment and the Test [redacted] environment, and to perform support of the [redacted] applications which live on the [redacted] servers in the ESP.

A thorough review was completed by EMS Security on 8/12/2016 that included an examination of [redacted] from July 1, 2016 – Aug 11, 2016 to understand the extent of the utilization, and to identify traffic utilizing [redacted] to access BES Cyber Systems within the ESP's without going through the IRA-IS solution. These reports were analyzed to determine source and destination of the traffic and also the user. The data was compiled and categorized into allowed and questionable access. [redacted] can be used for [redacted] and also [redacted] (which would not be Interactive Remote Access). Discussions were held with employees to determine how the port was utilized.

During the review, two additional employees were found to have also bypassed the IRA-IS system from outside the ESP when using a shared user account to [redacted] over [redacted] to access production [redacted] BES Cyber Assets within the ESP, and to perform support of the [redacted] applications. [redacted] and EMS [redacted] are both EMS High-Impact BES Cyber Systems that require support from outside the ESP. These two individuals are two of the nine users with authorized electronic access to this shared user account, and only these 2 of the 9 authorized users were improperly bypassing the IRA-IS solution. As a result, EMS is planning to implement additional measures to restrict unauthorized [redacted] usage over [redacted] into the ESP to enforce use of and remote access through the IRA-IS system.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

1) EMS will review [redacted] and conduct staff interviews to determine if any additional user [redacted] access over [redacted] occurred bypassing the IRA solution. Completed 8/12/2016
2) EMS will conduct training and provide instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP. Completed 9/20/2016
3) EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of [redacted] over [redacted] Completed 11/18/2016
4) EMS will complete the implementation of restricting [redacted] at [redacted] EMS ESPs, where possible as determined by a Tiger Team. Complete by 2/15/2017
5) EMS will complete the implementation of restricting [redacted] usage at the remaining [redacted] EMS ESPs, where possible as determined by a Tiger Team. Complete by 5/15/2017
6) EMS will complete updates to the EMS [redacted]' implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage. Complete by 7/1/2017

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will help prevent future recurrence of this issue.

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

7/1/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Review Logs	8/12/2016	1) EMS will review [redacted] and conduct staff interviews to determine if any additional user [redacted] access over [redacted] occurred bypassing the IRA solu ion.	No
Train Personnel	9/20/2016	2) EMS will conduct training and provide instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP.	No
Re-Train Personnel	11/18/2016	3) EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of [redacted] over [redacted]	Yes
Restrict Port Usage (50%)	2/15/2017	4) EMS will complete the implementation of restricting [redacted] at [redacted] EMS ESPs, where possible as determined by a Tiger Team.	Yes
Restrict Port Usage (100%)	5/15/2017	5) EMS will complete the implementation of restricting [redacted] usage at the remaining [redacted] EMS ESPs, where possible as determined by a Tiger Team.	Yes
Update [redacted] Implementation	7/1/2017	6) EMS will complete updates to the EMS [redacted]' implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage.	Yes

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:

This issue posed a moderate potential risk, and not a substantial potential risk to the bulk power system. In accordance with the CIP-005-5 R2 VRF of Medium, and VSL of Moderate, this issue involved not fully implementing processes to meet strict compliance with R2.1. Potential risk resulting from electronic access that bypasses the Intermediate System could include a possible compromise of the production EMS [redacted] or [redacted] systems by an EMS employee who had authorized electronic access to those test and production systems. While EMS staff have been instructed not to use [redacted] over [redacted] for performing support, tracking any access and actions performed though [redacted] is difficult and could prove improbable to trace back to an individual user in the event of a system compromise.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk and did not pose a serious or substantial actual risk to the reliability of the bulk power system. This issue was a result of three employees not following procedures implemented as of July 1, 2016 with regard to the use of the EMS IRA-IS for remote electronic access. Prior to 7/1/2016, EMS implemented the IRA-IS system based on [redacted] technology that controls and/or restricts remote access to only authorized users. All three of these users associated with this issue have a current Personnel Risk Assessment on file, had completed NERC CIP Cyber Security Training this year, and are current employees in good standing in EMS with active electronic access authorization to each of assets/systems relevant to this issue.

[redacted] While the three employees were able to directly access the production EMS [redacted] system from the test [redacted] system via [redacted] over [redacted] the employees also had to have authorization for Interactive Remote Access to access the test systems first from their EMS Desktops.

EMS relies upon its strong security strategy that includes infrastructure and security measures to mitigate vulnerabilities. [redacted]

Additional Comments:

[redacted] states in Section 4.2.2, Interactive Remote Access, "If Interactive Remote Access into the ESP is required, an Intermediate System shall be implemented such that the Cyber Asset initiating the access does not directly access the BES Cyber Systems or PCAs. The Intermediate System shall be outside or on the ESP; it cannot exist inside the ESP. Examples include remote desktop into a device outside or on the ESP, proxy servers, VPNs, or SSL VPNs that terminate on an EAP."

EMS Interactive Remote Access Work Practice states "EMS has implemented and maintains a process to ensure an Intermediate System is utilized such that a Cyber Asset initiating Interactive Remote Access (IRA) does not directly access applicable BES Cyber Systems or their associated PCAs." Section 4.1 details the requirements for EMS staff in the implementation and configuration of an IRA-IS. In this particular case, [redacted] was identified as a port needing to be enabled, and EMS had implemented an IRA-IS solution, but the capability for interactive user access from the Test system outside the ESP to the Production system inside the ESP, although both forms of access were originating from within the protected EMS network, could be considered directly accessing BES Cyber Systems from outside the ESP.

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)

VIEW FORMAL MITIGATION PLAN: CIP-005-5 (REGION REVIEWING MITIGATION PLAN)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 8/17/2018

This item was marked ready for signature by [redacted] on 8/16/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-005-5 R2.	SERC2016016548	SERC2016-402543	11/18/2016	Revision Requested	Informal	
CIP-005-5 R2.	SERC2016016548	SERC2016-402543	08/17/2018	Region reviewing Mitigation Plan	Formal	1

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: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	SERC2016-402543	SERC2016016548	11/18/2016

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

On 7/15/2016 an EMS employee discovered he was able to bypass the EMS Interactive Remote Access Intermediate System (IRA-IS) from outside the ESP when using [redacted] to access BES Cyber Assets within the ESP. CIP-005-5 R2.1 states the Responsible Entity shall: Utilize an Intermediate System such that he Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. The EMS employee, although authorized for electronic access to all of the following assets, was able to utilize an individual non-shared user account to [redacted] from the EMS [redacted], to the EMS [redacted] Upon discovery, the employee reported the issue to EMS Security for investigation. An initial investigation revealed the EMS employee did use the EMS IRA-IS to move from his EMS Desktop to the EMS [redacted] asset, but then used [redacted] to move directly from the EMS [redacted] asset outside the ESP to the EMS [redacted] asset within the ESP, bypassing the EMS IRA-IS system.

As of July 1, 2016, as part of the IRA-IS solution implementation, [redacted] was determined to be necessary for application usage for EMS [redacted] between the Production [redacted] environment and the Test [redacted] environment, and to perform support of the [redacted] applications which live on the [redacted] servers in the ESP.

A thorough review was completed by EMS Security on 8/12/2016 that included an examination of [redacted] from July 1, 2016 – Aug 11, 2016 to understand the extent of the utilization, and to identify traffic utilizing [redacted] to access BES Cyber Systems within the ESP's wi hout going through the IRA-IS solution. These reports were analyzed to determine source and destination of the traffic and also the user. The data was compiled and categorized into allowed and questionable access. [redacted] can be used for [redacted] and also [redacted] (which would not be Interactive Remote Access). Discussions were held with employees to determine how the port was utilized.

During the review, two additional employees were found to have also bypassed the IRA-IS system from outside the ESP when using a shared user account to [redacted] over [redacted] access produc ion [redacted] BES Cyber Assets within the ESP, and to perform support of the [redacted] applications. [redacted] and EMS [redacted] are both EMS High-Impact BES Cyber Systems that require support from outside the ESP. These two individuals are two of the nine users with authorized electronic access to this shared user account, and only these 2 of the 9 authorized users were improperly bypassing the IRA-IS solution. The last bypass occurred on August 10th, 2016. As a result, EMS has implemented additional measures to restrict unauthorized [redacted] usage over [redacted] into the ESP to enforce use of and remote access through the IRA-IS system.

There was no known harm that occurred as a result of this issue.

Attachments ()

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

[redacted]

In this case, firewall rules(s) were in place to allow [redacted] traffic, because [redacted] was necessary for the [redacted] application/machine access from the non-CIP [redacted] and [redacted] to the CIP [redacted] systems. EMS had documented procedural controls via policy for personnel to not use this access method for Interactive Remote Access. As part of the remediation plan, [redacted] restrictions were put in place and the configuration was augmented to block any remote user based on system naming conventions.

The number of sites, impact ratings, and Cyber Assets (type/classifications) that may have been impacted/affected are provided below, and includes the high impact BES Cyber Assets at each ESP that could have potentially been affected:

[redacted]

The numbers reflect the granular nature of the firewall rules the EMS group implements.

The apparent root-cause of this issue was a failure to implement adequate technical controls on or before July 1, 2016 to prevent remote access from bypassing the IRA system. Prior to July 1, 2016, EMS identified [redacted] as required, however the technical controls in place failed to ensure [redacted] was accessed only through the intermediate system.

The EMS group determined the extent-of-condition for this issue through mitigation step 1, which provided EMS will review [redacted] and conduct staff interviews to determine if any additional user [redacted] access over [redacted] occurred, bypassing the IRA solution. The review was completed on 8/12/2016 and resulted in the identification of [redacted] additional employees found to have also bypassed the IRA system from outside the ESP when using [redacted] over [redacted] to access production [redacted] BES Cyber Assets within the ESP.

The purpose of the review was to understand the extent of the utilization of the bypass, and to identify traffic utilizing [redacted] to access the ESP's. The reports were analyzed to determine source and destination of the traffic and also the user.

The data was compiled and categorized into allowed and questionable access. [redacted] can be used for [redacted] and also [redacted] (which would not be Interactive Remote Access). Discussions were held with employees to determine how the port was utilized. The review found, in addition to the initial bypass, two additional employees bypassed the IRA system from outside the ESP when using a shared user account to [redacted] over [redacted] to access production [redacted] BES Cyber Assets within the ESP.

[redacted]

As part of the [redacted] CIP Procedures Manual, [redacted] has implemented [redacted], [redacted] Procedure to address CIP-005-5 R2.1. [redacted] states in [redacted] Interactive Remote Access:
• "If Interactive Remote Access into the ESP is required, an Intermediate System shall be implemented such that the Cyber Asset initiating the access does not directly access the BES Cyber Systems or PCAs. The Intermediate System shall be outside or on the ESP; it cannot exist inside the ESP. Examples include remote desktop into a device outside or on the ESP, proxy servers, VPNs, or SSL VPNs that terminate on an EAP."
EMS also maintains the EMS Interactive Remote Access Work Practice, which states:
• "EMS has implemented and maintains a process to ensure an Intermediate System is utilized such that a Cyber Asset initiating Interactive Remote Access (IRA) does not directly access applicable BES Cyber Systems or their associated PCAs."
• Section 4.1 details the requirements for EMS staff in the implementation and configuration of an IRA-IS. In this particular case, [redacted] was identified as a port needing to be enabled, and EMS had implemented an IRA-IS solution, but the capability for interactive user access from the Test system outside the ESP to the Production system inside the ESP, although both forms of access were originating from within the protected EMS network, could be considered directly accessing BES Cyber Systems from outside the ESP.

This issue was not discovered through a formal internal controls process.

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:

Description of Mitigating Activities:
1) EMS will review [redacted] and conduct staff interviews to determine if any additional user [redacted] access over [redacted] occurred bypassing the IRA solution. Completed 8/12/2016
2) EMS will conduct training and provide instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP. Completed 9/20/2016
3) EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of [redacted] over [redacted] Completed 11/16/2016
4) EMS will complete the implementation of restricting [redacted] at [redacted] EMS ESPs, where possible as determined by a Tiger Team. Complete by 2/13/2017
5) EMS will complete the implementation of restricting [redacted] usage at the remaining [redacted] EMS ESPs, where possible as determined by a Tiger Team. Completed 5/12/2017
6) EMS will complete updates to the EMS [redacted] implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage. Completed 6/26/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will help prevent future recurrence of this issue.

NOT PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Attachments ()

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:

7/1/2017

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

Review Logs

Milestone Completed (Due: 8/12/2016 and Completed 8/12/2016)

1) EMS will review [redacted] and cond[redacted] to c[redacted] additi[redacted] [redacted]ss ove[redacted] occurred bypassing the IRA solu[redacted]

Train Personnel

Milestone Completed (Due: 9/20/2016 and Completed 9/20/2016)

2) EMS will conduc[redacted] provide in[redacted] taff[redacted] orde[redacted] er Sys[redacted] hin the ESP. [redacted]

Re-Train Personnel

Milestone Completed (Due: 11/18/2016 and Completed 11/16/2016)

3) EMS will conduc[redacted] ning/couns[redacted] EM[redacted] nauth[redacted] over[redacted] [redacted]

Restrict Port Usage (50%)

Milestone Completed (Due: 2/15/2017 and Completed 2/13/2017)

4) EMS will comple[redacted] entation o[redacted] at[redacted] EMS [redacted] le as [redacted] d by a Tiger Team. [redacted]

Restrict Port Usage (100%)

Milestone Completed (Due: 5/15/2017 and Completed 5/12/2017)

5) EMS will comple[redacted] entation o[redacted] us[redacted] aining [redacted] MS ES[redacted] e possible as determined by a Ti[redacted] eam.

Update SSHD Implementation

Milestone Completed (Due: 7/1/2017 and Completed 6/26/2017)

6) EMS will comple[redacted] the EMS [redacted] ple[redacted] strict [redacted] and w[redacted] onitor, and alert on unapproved [redacted] usage.

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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii) [redacted] does not plan to implement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed a minimal actual risk and did not pose a serious or substantial actual risk to the reliability of the bulk power system. This issue was a result of three employees not following procedures implemented as of July 1, 2016 with regard to the use of the EMS IRA-IS for remote electronic access. Prior to 7/1/2016, EMS implemented the IRA-IS system based on [redacted] technology that controls and/or restricts remote access to only authorized users. All three of these users associated with this issue have a current Personnel Risk Assessment on file, had completed NERC CIP Cyber Security Training this year, and are current employees in good standing in EMS with active electronic access authorization to each of assets/systems relevant to this issue.

[redacted] While the three employees were able to directly access the production EMS [redacted] system from the test [redacted] system via [redacted] over [redacted] the employees also had to have authorization for Interactive Remote Access to access the test systems first from their EMS Desktops.

EMS relies upon its strong security strategy that includes infrastructure and security measures to mitigate vulnerabilities. [redacted]

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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):

Successful completion of this mitigation plan will minimize the probability of future violations of the same requirements by restricting [redacted] usage between the EMS [redacted] [redacted] (backup) and [redacted] (production) systems, and by retraining personnel.

As noted in the originally submitted self-report, EMS has completed the following actions to prevent future recurrence:

2. EMS will conduct training and provide instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP.
• Completed 9/20/2016
3. EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of [redacted]
• Completed 11/16/2016
4. EMS will complete the implementation of restricting port 22 at [redacted] EMS ESPs, where possible as determined by a Tiger Team.
• Completed 2/13/2017
5. EMS will complete the implementation of restricting [redacted] usage at the remaining [redacted] EMS ESPs, where possible as determined by a Tiger Team.
• Completed 5/12/2017
6. EMS will complete updates to the EMS [redacted] implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage.
• Completed 6/26/2017

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 SERC 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 Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-005-5 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 8/17/2018

This item was marked ready for signature by [redacted] on 8/16/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R2.	SERC2016-402543	SERC2016016548

Date of completion of the Mitigation Plan:

[redacted]

Review Logs

Milestone Completed (Due: 8/12/2016 and Completed 8/12/2016)
Attachments (0)

1) EMS will review [redacted] and cond[redacted]te[redacted]to c[redacted] additi[redacted]ss ov[redacted] occurred bypassing the IRA solu[redacted].

Train Personnel

Milestone Completed (Due: 9/20/2016 and Completed 9/20/2016)
Attachments (0)

2) EMS will conduc[redacted] provide in[redacted] t[redacted]taff[redacted]h orde[redacted]er Sy[redacted]hin the ESP. [redacted]

Re-Train Personnel

Milestone Completed (Due: 11/18/2016 and Completed 11/16/2016)
Attachments (0)

3) EMS will conduc[redacted]ning/couns[redacted]si[redacted]EM[redacted]nauth[redacted] ove[redacted] [redacted]

Restrict Port Usage (50%)

Milestone Completed (Due: 2/15/2017 and Completed 2/13/2017)
Attachments (0)

4) EMS will comple[redacted]entation o[redacted]g[redacted] at[redacted] EMS [redacted]le as [redacted]ed by a Tiger Team. [redacted]

Restrict Port Usage (100%)

Milestone Completed (Due: 5/15/2017 and Completed 5/12/2017)
Attachments (0)

5) EMS will comple[redacted]entation o[redacted]ng[redacted] us[redacted]aining [redacted]MS ES[redacted]e possible as determined by a Ti[redacted]Team.

Update SSHD Implementation

Milestone Completed (Due: 7/1/2017 and Completed 6/26/2017)
Attachments (0)

6) EMS will comple[redacted] the EMS[redacted] '[redacted]ple[redacted]strict [redacted] and [redacted]onitor, and alert on unapproved[redacted] usage.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities:
1) EMS will review[redacted] logs and conduct staff interviews to determine if any additional user SSH access over[redacted] occurred bypassing the IRA solution. Completed 8/12/2016
2) EMS will conduct training and provide instructions to EMS staff on using IRA in order to access BES Cyber Systems within the ESP. Completed 9/20/2016
3) EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of[redacted] ove[redacted]. Completed 11/16/2016
4) EMS will complete the implementa ion of restricting[redacted] at[redacted] EMS ESPs, where possible as determined by a Tiger Team. Complete by 2/13/2017
5) EMS will complete the implementation of restricting[redacted] usage at the remaining[redacted] EMS ESPs, where possible as determined by a Tiger Team. Completed 5/12/2017

6) EMS will complete updates to the EMS [redacted] implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage.
Completed 6/26/2017

Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will help prevent future occurrence and is sufficient.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Description of the information provided to SERC for their evaluation *

Milestone 1:
EMS will review [redacted] logs and conduct staff interviews to determine if any additional user [redacted] access over [redacted] occurred bypassing the IRA solution.
Completed 8/12/2016
[redacted] Provides a summary of the analysis of the potential violation and extent of condition. As part of the analysis, employees were interviewed and a review of the [redacted] logs provided in the file: [redacted] was completed as of 8/12/2016.

Milestone 2:
EMS will conduct training and provide instructions to EMS staff on using IRA to access BES Cyber Systems within he ESP.
[redacted] provides emailed instructions to the EMS staff concerning the proper use of Interactive Remote Access provided on 8/12/2016. The instruction guide, [redacted] was provided as part of the email.
[redacted], provides the agenda for the EMS [redacted] update meeting conducted on 9/20/2017. As part of training, the following were reviewed: [redacted] provides he steps for granting, revoking, or modifying electronic access to EMS system [redacted] provides instruction for the commissioning of the IRA system.

Milestone 3:
EMS will conduct another training/counseling session with EMS staff on the unauthorized usage of [redacted] over [redacted]
Between 11/10/2016 and 11/16/2016, EMS conducted training sessions with EMS staff on the unauthorized usage if [redacted] over [redacted]
[redacted] provides the training presentation.
[redacted] provides the list of attendees.

The following provide the invitations for training:
[redacted] (11/10/2016 9:00am – 9:30am)
(11/10/2016 9:30am – 10:00am)
(11/14/2016 8:30am – 9:00am)
(11/14/2016 9:00am – 9:30am)
(11/15/2016 1:30pm – 2:00pm)
(11/16/2016 3:00pm – 3:30pm)

Milestone 4:
EMS will complete the implementation of restricting [redacted] at [redacted] EMS ESPs, where possible as determined by a Tiger Team.
[redacted] is a change request showing removal of [redacted] access over [redacted]. This is accomplished by removing the [redacted] and [redacted] objects from the [redacted] rule.
[redacted] f shows the initial systems changed to complete the milestone (at least [redacted] by 2/16/2017).
[redacted] shows the rule base with the [redacted] and [redacted] systems removed.

Milestone 5:
EMS will complete the implementation of restricting [redacted] usage at the remaining [redacted] EMS ESPs, where possible as determined by a Tiger Team.
[redacted] shows the remaining systems changed to complete this milestone (the remainder by 5/17/2017). N/A shows systems which could not be changed and are addressed in Milestone 6.

Milestone 6:
EMS will complete updates to the EMS [redacted] implementation to restrict user/system access, and will log, monitor, and alert on unapproved [redacted] usage.
[redacted] shows that [redacted] (the vendor of the EMS) requires [redacted] access on [redacted] systems and that existing firewall rules block [redacted] [redacted] s also configured to log and alerts on access attempts. On pages 2 through 6 of the file, the CR to implement restrictions via the [redacted] configuration file is shown. Pages 7 through 11 show a sample set of the systems tested with the rules in place.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 6

Record documents for the violation of CIP-006-6 R1

6a. The Entities' Self-Report (SERC2017017286)

6b. The Entities' Mitigation Plan designated as SERCMIT014400 submitted June 26, 2018

6c. The Entities' Certification of Mitigation Plan Completion submitted June 26, 2018

VIEW SELF-REPORT: CIP-006-6 R1. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 3/24/2017

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]
Applicable Requirement:	[redacted]
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:	1/31/2017
Beginning Date of Possible Violation:	12/6/2016
End or Expected End Date of Possible Violation:	1/31/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On January 31, 2017, [redacted] Corporate Security discovered a potential violation of CIP-006-6 R1.2 where an employee reported his badge as lost on December 5th, 2016. The lost badge was replaced and the new badge was updated in the [redacted] non-CIP badging system on December 5, 2016; however, his badge record was not updated with the new badge in the CIP PACS [redacted] system until January 31, 2017. The lost badge allowed access into [redacted] Transmission Substation switch houses containing Medium Impact BES Cyber Systems, [redacted] of which reside within a [redacted] perimeter with 24/7 security on-site to control physical access. [redacted] This issue was discovered when, on January 31, 2017, the employee could not gain access to one of the "Medium" Substation PSPs that he was authorized to access with his new badge, and during investigating the issue, it was discovered the new badge was not updated in CIP PACS [redacted] system back on December 5, 2016. Therefore, the old (lost) badge remained active in the CIP PACS [redacted] system for approximately 57 days, which could have potentially allowed physical access by unauthorized personnel that found the lost badge. An access log report was ran on the lost badge between the 12/5/16 thru 1/31/17 dates and the PACS access logs showed no activity or attempted access into any CIP PSP's. [redacted] is currently performing an extent-of-condition review [redacted] to determine if this issue has occurred at any other locations. Additionally, to mitigate this issue, [redacted] will implement additional technical or procedural controls [redacted] to prevent future recurrence of this issue.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] Security will review badge logs to confirm the lost badge was not used or attempted to be used to gain access after being reported lost and while remaining active in the CIP PACS badging system. (Completed 2/8/2017)
2) The [redacted] will improve the daily review process by creating a daily reconciliation report that lists employee badge changes in all of the [redacted] non-CIP badge systems and [redacted] generation plants and compare those badge numbers to a list of active CIP PACS badge numbers to identify any discrepancies and make updates. (Completed 3/23/2017)
3) [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary. (Complete by 3/31/2017)
4) Extent of Condition [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in the CIP PACS badging system. (Complete by 5/1/2017)
5) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure

packet for SERC review and settlement of this potential violation. (Complete by 5/22/2017).

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

5/22/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Procedure Review and Update	3/31/2017	[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary.	Yes
Extent of Condition Review	5/5/2017	[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in he CIP PACS badging system.	No
Portal Closure	5/19/2017	[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	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 issue posed a minimal potential risk, and not a serious or substantial potential risk to the bulk power system. The lost badge remained active for 57 days before being removed in the CIP PACS system. The active lost badge could have provided access to [redacted] Substation switch houses containing Medium-Impact BES Cyber Systems for an individual that could have potentially gained access through other physical layers of security in place, such as perimeter fencing or 24/7 plant security staff.

Provide detailed description of Actual Risk to Bulk Power System:

This issue posed a minimal actual risk, and not a serious or substantial actual risk to the bulk power system. The active lost badge could have provided access to only [redacted] Substation switch houses containing Medium-Impact BES Cyber Systems out of [redacted] total across [redacted] for an individual that could have potentially gained access through other physical layers of security in place, such as perimeter fencing or 24/7 plant security staff. [redacted] A review was conducted of the access logs of the lost badge and showed there was no access attempt made using the lost badge during the dates it was reported lost and when it was disabled in the CIP PACS badge system.

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)

VIEW FORMAL MITIGATION PLAN: CIP-006-6 (REGION REVIEWING MITIGATION PLAN)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 6/26/2018

This item was marked ready for signature by [redacted] on 6/21/2018

MITIGATION PLAN REVISIONS

Requirement	NERC Violation IDs	Regional Violation Ids	Date Submitted	Status	Type	Revision Number
CIP-006-6 R1.	SERC2017017286	SERC2017-402649	03/24/2017	Revision Requested	Informal	
CIP-006-6 R1.	SERC2017017286	SERC2017-402649	06/26/2018	Region reviewing Mitigation Plan	Formal	1

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: [redacted]

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	SERC2017-402649	SERC2017017286	3/24/2017

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

On January 31, 2017 [redacted] Corporate Security discovered a potential violation of CIP-006-6 R1.2 where an employee reported his badge as lost on December 5th, 2016. The lost badge was replaced and the new badge was updated in the [redacted] non-CIP badging system on December 5, 2016; however, his badge record was not updated with the new badge in the CIP PACS [redacted] system until January 31, 2017. The lost badge could have been used to access [redacted] Transmission Substation switch houses containing Medium Impact BES Cyber Systems, [redacted] of which reside within a [redacted] perimeter with 24/7 security on-site to control physical access. [redacted] This issue was discovered when, on January 31, 2017, the employee could not gain access to one of the "Medium" Substation PSPs that he was authorized to access with his new badge, and during investigating the issue, it was discovered the new badge was not updated in CIP PACS [redacted] system back on December 5, 2016. Therefore, the old (lost) badge remained active in the CIP PACS [redacted] system for approximately 57 days, which could have potentially allowed physical access by unauthorized personnel that found the lost badge. An access log report was run on the lost badge between the 12/5/16 thru 1/31/17 dates and the PACS access logs showed no activity or attempted access into any CIP PSP's.

The root cause of this issue was when a security analyst in the security badge office at [redacted] issued the employee a new badge and failed to follow the required process of adding a note in the non-CIP badging system identifying that the employee also has CIP access. The CIP access note would have triggered the security analyst to update (or notify [redacted] Corporate Security to update) the employee's badge in the CIP PACS badging system. By not adding the note, the needed badge number changes in the CIP PACS system were not made in a timely manner, which resulted in the lost badge remaining active in the CIP PACS system for 57 days.

As part of milestone 4 of the self-report, to determine the extent-of-condition for this issue, the [redacted] worked with each [redacted] security badge office to perform a badge system record reconciliation review to ensure that there are no additional lost badges that have been updated in the non-CIP badge system, while the lost badge remains active the CIP PACS system. The reconciliation review compared badge numbers of all personnel with authorized CIP access clearances in he CIP PACS system to their badge numbers in each individual [redacted] corporate security non-CIP badging system. The review identified [redacted] occurrences where an individual's badge number in the CIP PACS system did not match the badge number in the non-CIP badge system. Upon review and investigation, it was confirmed that each of the [redacted] occurrences were the result of the previous or old CIP badge being returned to an [redacted] badge office and being destroyed, thereby preventing the ability of unauthorized physical access to a CIP PSP, but where the updates in the CIP PACS system were delayed. There were no additional occurrences of a lost CIP badge being active in the CIP PACS system.

There was no known harm that occurred as a result of this issue.

Attachments ()

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

This issue involved a total number of [redacted] Transmission Substation BES Cyber Systems (individual BES Cyber Assets) and associated EACMS and PCAs at [redacted] out of a total of [redacted] across [redacted]. The [redacted] devices were protected within the [redacted] Substation switch house PSPs that the lost badge could have provided the capability to access if other Substation and Plant layers of security were also breached. The individual in question that lost his badge had no electronic or Interactive Remote Access to any BES Cyber Assets and his unescorted physical access (badge access) was limited to the [redacted] Substation switch house PSPs.

As part of the [redacted] CIP Procedures Manual, [redacted] has implemented the [redacted] to address CIP-006-6 R1.2 across [redacted]. [redacted] is an overarching procedure that documents and defines the processes required to be implemented and maintained for a compliant physical security program. Specifically, [redacted] on page [redacted] directs the actions that an authorized user is required to take for a lost badge.

Also as part of the CIP Procedures Manual, [redacted] Lost Badge Procedure defines the processes required to be implemented when an authorized user has lost a physical badge that provides access to a Physical Security Perimeter (PSP). Specifically, Section 4.0, on page 4 of [redacted] details the process for replacing an authorized user's lost badge. [redacted] defines the responsibilities of the [redacted] and [redacted] security when notified of a lost badge approved for access to a PSP.

In addition, the [redacted] developed a NERC CIP Badge Management Procedure that each [redacted] badge office uses as to ensure a consistent and repeatable process when an individual approved for access to a PSP requests a replacement badge.
This issue was not discovered through a formal internal controls process, but rather a chance event when an authorized user was denied badge access to a Substation PSP for which they had approval to access.

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:

Description of Mitigating Activities:
1) [redacted] Corporate Security will review badge logs to confirm the lost badge was not used or attempted to be used to gain access after being reported lost and while remaining active in the CIP PACS badging system. (Completed 2/8/2017)
2) The [redacted] will improve the daily review process by creating a daily reconciliation report that lists employee badge changes in all of the [redacted] non-CIP badge systems and [redacted] generation plants and compare those badge numbers to a list of active CIP PACS badge numbers to identify any discrepancies and make updates. (Completed 3/23/2017)
3) [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary. (Completed 3/27/2017)
4) Extent of Condition: [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in the CIP PACS badging system. (Completed 4/27/2017)
5) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. (Completed 5/1/2017).

Attachments ()

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:

5/19/2017

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

Procedure Review and Update

Milestone Completed (Due: 3/31/2017 and Completed 3/27/2017)

[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary.

Extent of Condition Review

Milestone Completed (Due: 5/5/2017 and Completed 4/27/2017)

[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in the CIP PACS badging system.

Portal Closure

Milestone Completed (Due: 5/19/2017 and Completed 5/1/2017)

[redacted] Operations Compliance w[redacted]mplete a comprehen[redacted]eview of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.

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):

(i) There are no known additional risks or impacts to the BPS while the actions in this mitigation plan are being completed.
(ii) [redacted] does not plan to implement additional actions that would increase risks to the reliability of the BPS as part of this mitigation plan.

[redacted] assesses this issue posed a minimal actual risk, and not a serious or substantial risk to the reliability of the bulk electric system. The active lost badge could have provided access to only [redacted] Substation switch houses containing Medium-Impact BES Cyber Systems out of [redacted] total across [redacted] If an individual recovered the lost badge, there were other physical layers of security in place, such as perimeter fencing or 24/7 plant security staff. [redacted] c[redacted]

[redacted] A review was conducted of the access logs of the lost badge and showed there was no access attempt made using the lost badge between the date it was lost and the date it was disabled in the CIP PACS badge system.

NON-PUBLIC AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Attachments ()

E.2 Prevention of Future BPS Reliability Risk: Describe how successful completion of this Mitiga ion 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):

Successful completion of this mitigation plan will minimize the probability of future violations of the same requirements by adding additional controls to perform a daily review of corporate badge changes compared against badge credentials in the CIP PACS system to ensure badge numbers stay in sync, and by reinforcing with each of the OPCO badge offices the steps for making badge updates for personnel with CIP access.
As noted in the originally submitted self-report, the [redacted] and [redacted] Corporate Security have completed the following actions to prevent future recurrence:
2) The [redacted] will improve the daily review process by creating a daily reconciliation report that lists employee badge changes in all of the [redacted] non-CIP badge systems and [redacted] generation plants and compare those badge numbers to a list of active CIP PACS badge numbers to identify any discrepancies and make updates. (Completed 3/23/2017)
3) [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary. (Completed 3/27/2017)

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 SERC 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 Appendixe 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 SERC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

SERC Single Point of Contact (SPOC)

VIEW MITIGATION PLAN CLOSURE: CIP-006-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 6/26/2018

This item was marked ready for signature by [redacted] on 6/21/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R1.	SERC2017-402649	SERC2017017286

Date of completion of the Mitigation Plan:

[redacted]

Procedure Review and Update

Milestone Completed (Due: 3/31/2017 and Completed 3/27/2017)
Attachments (0)

[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary.

Extent of Condition Review

Milestone Completed (Due: 5/5/2017 and Completed 4/27/2017)
Attachments (0)

[redacted] Ops Compliance and the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in the CIP PACS badging system.

Portal Closure

Milestone Completed (Due: 5/19/2017 and Completed 5/1/2017)
Attachments (0)

[redacted] Operations Compliance w[redacted]mplete a comprehen[redacted]eview of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities:
1) [redacted] Security will review badge logs to confirm the lost badge was not used or attempted to be used to gain access after being reported lost and while remaining active in the CIP PACS badging system. (Completed 2/8/2017)
2) The [redacted] will improve the daily review process by creating a daily reconciliation report that lists employee badge changes in all of the OpCo non-CIP badge systems and [redacted] generation plants and compare those badge numbers to a list of active CIP PACS badge numbers to identify any discrepancies and make updates. (Completed 3/23/2017)
3) [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a review of badge office procedures for responding to lost badges and updating the CIP PACS badge system, and make updates where necessary. (Completed 3/27/2017)
4) Extent of Condition: [redacted] Ops Compliance & the [redacted] will work with each [redacted] badge office to perform a badge system records reconciliation review to ensure there are no additional lost badges updated in a non-CIP badge system that remain active in the CIP PACS badging system. (Completed 4/27/2017)
5) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. (Completed 5/1/2017).

Description of the information provided to SERC for their evaluation *

Milestone 1:
[redacted] shows a description from [redacted] Corporate Security personnel of the potential lost badge update issue, and screenshots from the CIP Physical Access Control System (PACS) [redacted] that demonstrates no access attempts had been made using the employee's lost badge between 12/5/2016 and 1/31/2017 – the timeframe that the badge was lost and not updated in the CIP PACS system.

Milestone 2:
[redacted] shows an example of the daily badge report reconciliation comparing all system badge changes to badge records in CIP PACS to ensure there are no badge discrepancies.

Milestone 3:

[redacted] shows the revised NERC CIP Badge Management Procedure, dated March 20, 2017, providing direction to each [redacted] Corporate Security Badge Office and the [redacted] for responding to lost badges . The highlighted sections reflect changes implemented in the revised procedure in response to this self-report.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[redacted] shows the previous version of the NERC CIP Badge Management Procedure effective April 20, 2016 prior to the revisions and updates in the NERC CIP Badge Management Procedure, dated March 20, 2017.

[redacted] demonstrates the dissemination on 3/20/2017 of the revised NERC CIP Badge Management Procedure to each [redacted] Corporate Security contact, and subsequent responses for all applicable personnel that the updated procedure had been communicated and reinforced with all badge administrators.

Milestone 4:

[redacted] reconciliation and review completed on 4/27/2017 of the extent of condition to determine if any there were any other individuals who had an occurrence of a lost or unaccounted badge that was not disabled or updated in the CIP PACS instance in a timely manner. The review is comparing the badge numbers of personnel with authorized CIP clearances in the CIP PACS [redacted] to their badge numbers in each individual [redacted] ([redacted] Corporate Security non-CIP badge system. The review determined [redacted] occurrences where the individual's badge number in the CIP PACS system did not match the badge number in the non-CIP badge system; however, each individual occurrence was researched by the applicable [redacted] Corporate Security team and confirmed that each of the [redacted] occurrences were the result of the "old" CIP badge being returned to a badge office and destroyed, and the updates in the CIP PACS system were delayed.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 7

Record documents for the violation of CIP-006-6 R2

7a. The Entities' Self-Report (SERC2017018440)

7b. The Entities' Certification of Mitigation Plan Completion submitted January 23, 2018

7c. The Entities' Self-Report (SERC2017018441)

7d. The Entities' Certification of Mitigation Plan Completion submitted April 18, 2019

VIEW SELF-REPORT: CIP-006-6 R2. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 10/6/2017

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:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
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):

SERC ID SERC2017-402867

Date Reported to Region or Discovered by Region:

10/6/2017

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: 7/18/2017

Beginning Date of Possible Violation: 4/20/2017

End or Expected End Date of Possible Violation: 8/10/2017

Is the violation still occurring? No

Provide detailed description and cause of Possible Violation:

On 3/21/2017, members of the [redacted] Team ([redacted] discovered a potential violation of CIP-006-6 R2.2 when they were on-site at an [redacted] Transmission Substation containing Medium Impact BES Cyber Systems conducting physical site assessments as per CIP-006-6 R3. During the site assessment, the [redacted] members noted a missing "Time Out" entry in the visitor log book for the date of 2/1/2017.

This visitor log book issue at [redacted] (self-reported as SERC Issue [redacted]) was reported to [redacted] Operations Compliance by [redacted] Transmission Compliance on 6/7/2017, and an extent-of-condition review was initiated using CIP Internal Controls sampling methodology to randomly sample and review [redacted] PSP visitor log books out of a total population of [redacted] PSPs across [redacted]. As of 7/18/2017, each of the [redacted] sampled [redacted] PSP visitor log books were reviewed to determine if any additional errors existed.

During the extent-of-condition review of SERC Issue [redacted], two visitor log book issues resulting from missing information in the [redacted] PSP visitor log book were identified on 7/18/2017. Both visitor log book issues occurred on 4/20/2017, and were the responsibility of the same person acting as the escort. Visitor log book error #1 at the [redacted] was a failure of the escort to provide the escort name in the visitor log book. The escort was escorting a contract cleaning vendor that entered the [redacted] at 8:45pm and exited he [redacted] at 9:08pm. Visitor log book error #2 at the [redacted] was a failure by the same escort to log a time of exit for a contract cleaning vendor that entered the [redacted] at 9:14pm. Using he Physical Access Control System (PACS), it was determined hat the escort exited the [redacted] with the visitor at 9:23pm. Using video camera footage as an investigative tool to corroborate both log book errors, it was determined who the escort was and that the escort remained with both escorted visitors at all times while within the [redacted]

While investigating and mitigating these two issues, two additional visitor control issues at the [redacted] were discovered. Visitor control issue #1 was discovered on 8/2/2017 involving a visitor that was not continuously escorted within the [redacted] by a [redacted] employee #1. On 8/2/2017, another [redacted] employee #2 saw an individual whom

the employee knew to be a visitor sitting alone in [redacted] employee #1's office. The [redacted] employee #2 stopped and questioned the visitor about their escort. The [redacted] employee #2 immediately took escort responsibility for the visitor and escorted the visitor out of the [redacted] area. The visitor logged in the [redacted] log book at 7:26am and is a student co-op that had entered the [redacted] to conduct required work activities. The visitor's escort was a [redacted] employee #1 that mistakenly left the visitor unattended in the office area for less than five minutes so that the escort could leave the office area to use the restroom. The office area where the visitor was left alone is not the actual control center area of the PSP where the control center BES Cyber Systems reside for control purposes.

NON-PUBLIC AND/OR CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Visitor control issue #2 at the [redacted] was discovered on 8/10/2017 when an authorized [redacted] facilities contractor (escort) did not continuously escort a second unauthorized cleaning crew contractor (visitor) while within the [redacted] PSP to perform cleaning and restocking in the breakroom. On 8/10/2017 at approximately 7:00pm, a [redacted] employee noticed the visitor standing alone in the breakroom and questioned the visitor about their escort. The [redacted] employee immediately took escort responsibility for the visitor and took the visitor to find their original escort. The visitor logged in the [redacted] log book at 6:55pm, so the visitor was unescorted for approximately five minutes. The breakroom area where the visitor was out of the line of sight of the escort is in an area outside of the actual control center area of the PSP where the control center BES Cyber Systems reside for control purposes.

To mitigate and correct these visitor control issues:
1[redacted] Transmission Compliance conducted a CIP visitor control refresher training for [redacted] employees on the afternoon of 8/2/2017, covering visitor log book requirements and escort responsibilities when escorting visitors within a PSP. The [redacted] employee #1 that was responsible for visitor control issue #1 and leaving the student visitor alone attended the retraining session.

To prevent future recurrence of these visitor escort and logging issues:
2. [redacted] Operations Compliance will include reinforcement in the Q3 Cyber Security Awareness Newsletter covering visitor log book completion and escort responsibility sent to all personnel with CIP unescorted physical access by 9/30/2017.
3. [redacted] Transmission Compliance will also administer required in-person training on CIP visitor control by 10/10/2017 for all employees and contractors working in the [redacted], covering visitor log book requirements and escort responsibilities when escorting visitors within a PSP.
4. [redacted] Transmission Compliance will also administer required in-person training on CIP visitor control by 10/10/2017 for [redacted] Corporate Facilities employees and personnel working for the contract cleaning crew vendor, covering visitor log book requirements and escort responsibilities when escorting visitors within a PSP.

The root cause of these visitor log and escorting issues is a lack of adherence to [redacted] procedure [redacted], Visitor Control Program (CIP-006-6 R2) and visitor control training received annually in CIP Cyber Security Training as per CIP-004-6 R2. Preventative measures to address these escorting issues will include the loss of unescorted physical access for the personnel found not complying with [redacted] until CIP Cyber Security Training is retaken and/or the individuals have reported to [redacted] management the requirements of proper visitor access controls.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] Ops Compliance and each [redacted] and [redacted] business unit shall perform an extent-of-condition review of a random sample of [redacted] PSP visitor log books to determine if any additional log book issues exist. Completed 07/28/2017
2) [redacted] Ops Compliance shall disseminate additional reinforcement on [redacted], CIP Visitor Control Program in the CIP quarterly awareness newsletter on proper escorting and logging responsibilities. Completed 9/30/2017
3) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in the [redacted] with authorized unescorted physical access to the [redacted]. The refresher training will be completed by 10/10/2017.
4) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] Corporate Facilities and personnel working for the contract cleaning vendor with authorized unescorted physical access to the [redacted]. The refresher training will be completed by 10/20/2017.
5) [redacted] Operations Compliance shall produce a comprehensive closure package. Completed by 10/27/2017

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

10/27/2017

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
In Person [redacted] Retraining	10/13/2017	3) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in the [redacted] with authorized unescorted physical access to the [redacted] The refresher training will be completed by 10/10/2017.	Yes
In Person Facilities Retraining	10/20/2017	4) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] Corporate Facilities and personnel working for the contract cleaning vendor with authorized unescorted physical access to the [redacted]. The refresher training will be completed by 10/20/2017.	Yes
Closure Package	10/27/2017	5) [redacted] Operations Compliance shall produce a comprehensive closure package. 10/27/2017	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:

These issues posed a minimal potential risk, and did not pose a serious or substantial risk to the BES. Improper logging of visitor access, which is a manual log book process at all [redacted] PSPs, provides after-the-fact investigative documentation of visitor access within a PSP with little to no real-time impact to the BES. The contract cleaning crews associated with the visitor logging issues remained within a segmented portion of the PSP outside of the actual control center in an office area of the [redacted] and were properly escorted throughout the duration they were within the PSP. However, failing to properly log visitors in accordance with established policy could demonstrate a lack of positive control of visitors within he PSP. Improper escorting of visitors within the PSP could have a higher degree of impact if visitors within the PSP are unaccounted for, and demonstrates a lack of adherence to established policy. With the issues of visitor escorting, the visitors in question were (#1) a student intern who was in the process of obtaining authorization for unescorted physical access to work in the [redacted], and was outside the line-of-sight of his escort for less than five minutes while he waited in the escort's office; the second (#2) was a member of a contracted vendor cleaning crew who is routinely in the [redacted] PSP, and the escort on this particular day lapsed in the performance of their escort responsibilities. Again, in all of these instances, these visitors were in an office area of the PSP and could not have accessed the control room where control center cyber assets reside.

Provide detailed description of Actual Risk to Bulk Power System:

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

These issues posed a minimal actual risk, and did not pose a serious or substantial risk to the BES. For the two visitor logging issues, the escort did not fully complete the two visitor log book entries for the contract cleaning crew members, but they did continuously escort the visitors while working in the [redacted]. Investigative footage confirmed the presence of the escort for the duration, and that the visitors exited the [redacted] PSP with their escort. The visitor log book errors are considered performance/attention-to-detail documentation errors.

The visitor escorting issues are considered minimal risk because the visitors in question were (#1) a student intern who was in the process of obtaining authorization for unescorted physical access to work in the [redacted], and was outside the line-of-sight of his escort for less than five minutes while he waited in the escort's office; the second (#2) was a member of a contracted vendor cleaning crew who is routinely in the [redacted] PSP, and the escort on this particular day lapsed in the performance of their escort responsibilities for approximately five minutes. Again, in all of these instances, these visitors were in an office area of the PSP and could not have accessed the control room where control center cyber assets reside. [redacted] and [redacted] management do not believe that improper visitor logging and escorting is a pervasive issue, and that targeted visitor control refresher training and communication will reinforce the importance of ensuring visitors are properly logged and escorted within a PSP.

Additional Comments:

[redacted] has a CIP Visitor Control Program [redacted] which states:

[redacted] Visitor Control Program
Section 4.1.1 Continuous Escort of Visitors
Any personnel not authorized for unescorted physical access to a specific CIP PSP through an approved Company Access Management Application (AMA) shall be considered a Visitor and shall be continuously escorted until unescorted physical access is appropriately authorized. For situations where an individual is appropriately authorized while inside a PSP, the individual must remain escorted until they have been properly signed out in the visitor access log, exit the PSP and then re-enter the PSP using his/her own credentials.

Only Authorized Users to a specific CIP PSP can act as an Escort for Visitors to that PSP. When escorting a Visitor, Authorized Users shall meet all Visitors at a PSP access point and maintain line-of-sight observation of Visitors at all times within a CIP PSP.

Visitor badges issued by a respective [redacted] Security Badge Office shall not be assigned any physical access privileges (such as clearances) for any CIP PSP access points. At CIP PSPs where visitor identification badges are utilized and available, Visitors shall display those badges on outer clothing at waist level or above.

Sec ion 4.1.2 Logging of Visitor Access
All Visitor access to a CIP PSP shall be logged via automated or manual means upon initial entry and final exit of a PSP access point, per day or shift. Where automated logging is not available, a manual visitor log shall be used.

The Authorized User(s) providing escort functions for a Visitor is responsible for ensuring all Visitor access to a CIP PSP is properly logged, to include date and time of the Visitor's initial entry into and final exit from the PSP, the Visitor's full first and last name, the reason for the visit, and the full first and last name of an individual point of contact responsible for the Visitor.

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)

VIEW MITIGATION PLAN CLOSURE: CIP-006-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 1/23/2018

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R2.	SERC2017-402867	SERC2017018440

Date of completion of the Mitigation Plan:

[redacted]

Baseline Config Review

Milestone Completed (Due: 10/27/2017 and Completed 9/19/2017)
Attachments (0)

8) [redacted] and [redacted] Protection and Co[redacted]ll verify through a review of before and after baseline configurations of devices in the substation that while the visitor was unescorted, they did not attempt to access and did not make any changes to any CIP systems while in the substation.

CVA Review

Milestone Completed (Due: 10/27/2017 and Completed 10/18/2017)
Attachments (0)

9[redacted] and [redacted] Protection and Co[redacted]ill complete a CVA for all applicable CIP systems within the substation to confirm no unauthorized changes were made to devices within the substation.

Subs Signage

Milestone Completed (Due: 1/15/2018 and Completed 1/11/2018)
Attachments (0)

10[redacted] hav[redacted]nage added to the [redacted] Medium substation PSPs providing reinforcement to on-site personnel on visitor escorting and logging responsibilities.

Closure Package

Milestone Completed (Due: 1/31/2018 and Completed 1/23/2018)
Attachments (0)

11[redacted]mpre[redacted]ive review of all re[redacted]vidence associated with this mitigation plan and prepare a summary closure packet for SERC review and set lement of this potential violation.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities:
1[redacted] Transmission Compliance will conduct retraining sessions with the responsible escort to review [redacted], [redacted] and reinforce proper escort logging responsibilities. Completed 5/4/2017
2) [redacted] Ops Compliance and [redacted] shall perform an extent-of-condition review of ninety days' worth of a random sample of Company PSPs to determine if additional PSP visitor log book issues exist. Completed 7/18/2017
3) Transmission Maintenance General Manager will conduct a [redacted] review session with their direct reports to emphasize the importance of compliance with the CIP Visitor Control Program. Completed 7/24/2017
4) The Crew Foremen in [redacted] will conduct a review session with their direct reports, including the employee in question, to emphasize the importance of compliance with the CIP Visitor Control Program. Completed 7/25/2017
5) [redacted] Transmission Compliance will notify managers / supervisors that have direct reports with [redacted] CIP Substation unescorted badge access and instruct them on the NERC CIP visitor escort requirements. Completed 7/31/2017
6) The [redacted] shall conduct and complete their biennial review of Substation PSPs and report back any additional log book issues found. Completed 8/18/2017
7) [redacted] Ops Compliance shall produce and disseminate additional reinforcement on [redacted] in the Q3 CIP Cyber Security awareness newsletter on proper escorting and logging responsibilities. Completed 9/14/2017
8[redacted] [redacted] and [redacted] Protection and Controls will verify through a review of before and after baseline configurations of devices in the substation that while the visitor was unescorted, they did not attempt to access and did not make any changes to any CIP systems while in the substation. Completed by 10/27/2017
9[redacted] [redacted] and [redacted] Protection and Controls will complete a CVA for all applicable CIP systems within the substation to confirm no unauthorized changes were made to devices within the substation. Completed by 10/27/2017
10[redacted] Transmission Compliance will develop and have signage added to the [redacted] [redacted] Medium substation PSPs providing reinforcement to on-site personnel on visitor escorting and logging responsibilities. Completed by 1/15/2018
11[redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure

packet for SERC review and settlement of this potential violation. Completed by 1/31/2018

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Description of the information provided to SERC for their evaluation *

Closure Packet: [redacted] Fail to Escort & Log[redacted]

MS1:
[redacted] shows where [redacted] Transmission Compliance met with the Substation Crew Leader to discuss visitor logging and escort responsibilities. The Crew Leader took an action item to review this information with his staff at an upcoming staff meeting.
MS2:
[redacted] shows the PSP log book review random sample locations and results of the review. Issues noted were either those found as part of this self-report or were self-reported under another operating company [redacted]).
[redacted] shows the [redacted] logbook issue. The two entries on 02/01/2017 did not have a time out as required in [redacted] Section 4.1.2, Logging of Visitor Access.
[redacted] shows the [redacted] logbook issue. The entries on 06/07/2017 for [redacted]. employees [redacted] were both missing the responsible point of contact as required in [redacted], Section 4.1.2, Logging of Visitor Access. It was subsequently discovered after further review, that there was a third visitor, [redacted] who was not logged as a visitor, yet performed work on [redacted] owned equipment collocated in the substation on the same day.
MS3:
[redacted] is the meeting notice for a mandatory [redacted] led by the General Manager of the [redacted] Transmission Maintenance organization. At this meeting, the General Manager of the [redacted] Transmission Maintenance organization reviewed the [redacted] Visitor Control Program outlined in [redacted]
[redacted] shows the meeting minutes for a Maintenance Compliance group [redacted] where the General Manager of the [redacted] Transmission Maintenance organization addressed all of her direct reports (Managers and Supervisors in the same group) regarding NERC CIP escorting of visitors, and the associated requirements and responsibilities for escorts.
[redacted]; shows the [redacted] which outlines the requirements for both escorting and logging visitor access to facilities which house High-Impact or Medium-Impact BES Cyber Systems.
MS4:
[redacted] shows where the [redacted] Manager / Foreman addressed the offending escort employee as well as the rest of his crew regarding the requirements around NERC CIP unescorted physical badge access and the responsibilities of those escorting visitors.
MS5:
[redacted] shows the [redacted] Transmission Compliance Notification to all Supervisors and Managers within the [redacted] Transmission organization who have direct reports with [redacted] Substation NERC CIP unescorted badge access.
MS6:
[redacted] shows the [redacted] process for performing a "CIP-006-6 R3 Maintenance and Testing Review" and results for the 2017[redacted] tests.
MS7:
[redacted] shows the Q3 NERC CIP Cyber Awareness Newsletter sent to all [redacted] and [redacted] personnel with NERC CIP responsibilities. CIP Visitor Control is featured in this edition.
MS8:
[redacted] the meeting invitation for discussing the needed baseline review.
[redacted] is a summary of the Substations baseline verification from September 2017. Column A lists the applicable devices in the Substation, Column D shows the applicable baseline reference of record, Column E shows the results of the baseline confirmation, and Column F shows the network ID of the [redacted] /Field Services personnel performing the baseline verification.
[redacted] shows the host based firewall rules on the [redacted] logger device in the [redacted] Substation.
[redacted] shows the host based firewall rules on the HMI in the [redacted] Substation.
[redacted] shows the list of authorized open ports (baseline) on the TCP server devices in the [redacted] Substation.
[redacted] shows details from the [redacted] discovery on the HMI device in the [redacted] Substation. The reports shows that the ports listening are covered in the host based firewall, and therefore should be listening for proper operation. See [redacted] for comparison.

[redacted] shows details from the [redacted] discovery on the [redacted] device in the [redacted] Substation. The reports shows that the ports listening are covered in the host based firewall, and therefore should be listening for proper operation. See [redacted] for comparison.
[redacted] shows the device firmware versions for the devices in the [redacted] Substation.
[redacted] shows the OS, patches, software and host based firewall rules for the HMI and [redacted] devices in the [redacted] Substation.
[redacted] is the annual review of the baseline that was matched against in the baseline review.
MS9:
[redacted] is a confirmation from the [redacted] Supervisor that a member of her team went to [redacted] to gather the information that was only locally available such as serial device firmware. They also performed a visual verification of the network connections since the devices at this substation are primarily serial based devices.
[redacted] is the results of a (previous) vulnerability assessment for the [redacted] Substation.
[redacted] is the results of a vulnerability assessment for the [redacted] Substation.
MS10:
[redacted] shows the newly installed signage at all [redacted] Medium Impact substations reminding users of visitor and TCA requirements ("Electronic Requirements"). In this file, the first image shows the information on the signage. The second image shows the signage, as posted above the Visitor Log at an [redacted] Medium Impact BES facility. The Third image shows the signage in a desk work area. The fourth image shows the signage as mounted inside a rack next to a designated TCA laptop. The fifth image shows the signage on a substation door. The sixth image shows the signage on another substation door.
MS11:
See this closure packet.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

VIEW SELF-REPORT: CIP-006-6 R2. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was submitted by [redacted] on 10/6/2017

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:	[redacted]
NERC Registry ID:	[redacted]
JRO ID:	[redacted]
CFR ID:	[redacted]
Entity Contact Information:	[redacted]

REPORTING INFORMATION

Applicable Standard:	[redacted]
Applicable Requirement:	[redacted]
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:	3/21/2017
Beginning Date of Possible Violation:	2/1/2017
End or Expected End Date of Possible Violation:	4/20/2017
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On 3/21/2017, members of the CIP [redacted] Team ([redacted]) discovered a potential violation of CIP-006-6 R2.2 when they were on-site at a Transmission Substation containing Medium Impact BES Cyber Systems and noted a missing "Time Out" entry in the visitor log book for 2/1/2017 ("Original Issue"). This issue was reported to [redacted] Operations Compliance by [redacted] Transmission Compliance on 6/7/2017 and an extent-of-condition review was initiated using CIP Internal Controls sampling methodology of [redacted] PSP visitor log books out of [redacted] total PSPs across [redacted] (inclusive of affiliate operating companies).

Investigative footage and records from video surveillance of the Substation and from the PACS ([redacted]) system confirmed the visitors were properly escorted into and out of the PSP, and the time of exit for the visitors and their escort was confirmed through surveillance footage and badge logs in the PACS system. [redacted] Transmission Compliance conducted re-training with the escort at issue on 05/04/2017 to reinforce proper escort responsibilities and proper visitor logging. The escort in this issue also confirmed, at that time, that the visitors were properly escorted into and out of the PSP and that the manual visitor log entry was mistakenly overlooked. As part of the extent-of-condition review using sampling of an additional [redacted] random PSPs out of [redacted] total PSPs, copies of each of the PSP visitor log books were reviewed to determine if any additional errors existed. A regularly scheduled biennial review of PSPs was also performed. As of 7/18/2017 all [redacted] of the randomly sampled PSPs ([redacted] sampled, and the original PSP at issue) were reviewed with no additional instances of missing required information as per [redacted] procedure [redacted] Visitor Control Program.

During the biennial review of Medium Substations as per CIP-006-6 R3, which concluded 08/18/2017, another issue dealing with improper escorting and logging of visitors was discovered on 7/14/2017. On 6/7/2017 at another [redacted] Transmission Substation with Medium Impact BES Cyber Systems, an [redacted] employee (escort) failed to provide continuous escorted access of a visitor not authorized for unescorted physical access within the PSP. Additionally, it was discovered through investigation that the escort also did not properly log visitor access of three visitors that entered the Substation PSP on 6/7/2017. During the investigation, it was determined between the hours of 8:24am and 4:39pm, visitor (1) was in the PSP approximately 6 hours and 42 minutes, but the escort was only inside the PSP with the visitor approximately 1 hours 17 minutes. Therefore, the visitor remained inside the PSP unescorted for approximately 5 hours and 22 minutes. While the visitor was unescorted, the escort left the PSP to perform tasks outside of the PSP, but within the substation facility (yard), not in adherence to [redacted] Visitor Control Program, Section [redacted] "When escorting a Visitor, Authorized Users shall meet all Visitors at a PSP access point and maintain line-of-sight observation of Visitors at all times within a CIP PSP".

The visitor (1) is an employee of a third-party energy company (vendor) that owns a generator which has an interconnect at the substation. Annually, the vendor requests escorted access to the substation switch house to review data from the vendor owned watt-hour meters located inside the switch house to complete "capacity and heat rate" testing. The vendor owned meters are not BES Cyber Assets. These tests require a vendor employee to monitor the vendor owned watt-hour meters and manually document the meter readings every 10 minutes between approximately 9:00am and 5:00pm. This particular substation was previously not in-scope of the CIP Standards under Version 3, and came into scope July 1, 2016 under Version 5 as a "Medium" facility. The vendor employee does not have electronic access to any BES Cyber Assets/Systems within any Medium substation facility.

This investigation also revealed that the same [redacted] employee (escort) failed to properly log the entry of visitor (1) and two other visitor's access to the same Substation PSP on 6/7/2017. [redacted] uses manual visitor log books at all of its PSPs, and per [redacted] Visitor Control Program, requires entry of the date and time of the initial entry and last exit, the visitor's name, the purpose for the visit, and the name of an individual point of contact responsible for the visitor. Between 8:24am and 9:25am on 6/7/2017, the three visitors entered the PSP; visitor (1) was provided access to the PSP wi hout being properly escorted, visitor (2) and visitor (3) were provided

access to the PSP and were properly escorted in the PSP, but all three visitor's entry and exit of the PSP were not properly logged in the visitor log book.

The root cause of the issues related to CIP-006-6 R2.1 (failure to properly escort visitors in a CIP PSP) was a human performance error that resulted in the escort not remaining in the PSP and maintaining line-of-site observation of the visitor at all times. The escort left the visitor in the PSP unescorted and focused on other activities while the vendor was documenting testing information. The root cause of the issues related to CIP-006-6 R2.2 (failure to properly log visitor access to a CIP PSP) was human performance errors on the part of the authorized escorts in completing the visitor log book entries upon entry and exit of escorted visitors in a CIP PSP. In both cases, this was a failure to follow [redacted], Visitor Control Program. Specifically, section 4.4.1, page 2, of the procedure addresses continuous escort of visitors applicable to CIP-006-6 R2.1, and section 4.1.2, page 3, of the procedure addresses logging of visitor access applicable to CIP-006-6 R2.2.

NERC PUBLIC AND NON-CRITICAL ENERGY INFRASTRUCTURE INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

For the improper escorting issue, a technical assessment was performed on all of the BES Cyber Assets/Systems at the substation to verify there had been no attempted access or attempted changes to existing baseline configurations. No changes were noted that could not be accounted for as authorized in existing change management cases. A cyber vulnerability assessment was also performed at this substation and no anomalies were detected. To prevent future recurrence of these issues, [redacted] Transmission Compliance conducted retraining with the escorts involved in each incident. [redacted] Transmission Compliance and [redacted] Transmission leadership issued a maintenance [redacted] to address these issues with managers, and [redacted] quickly issued an awareness communications to the affected groups. [redacted] Operations Compliance has also included visitor logging and escort reinforcement guidance in the Q3 CIP Cyber Security Awareness newsletter which is sent to all personnel with CIP unescorted physical access.

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] Transmission Compliance will conduct retraining sessions with the responsible escort to review [redacted] Visitor Control Program and reinforce proper escort logging responsibilities. Completed 5/4/2017
2) [redacted] Ops Compliance and [redacted] shall perform an extent-of-condition review of ninety days' worth of a random sample of Company PSPs to determine if additional PSP visitor log book issues exist. Completed 7/18/2017
3) Transmission Maintenance General Manager will conduct a [redacted] review session with their direct reports to emphasize the importance of compliance with the CIP Visitor Control Program. Completed 7/24/2017
4) The Crew Foremen in [redacted] will conduct a review session with their direct reports, including the employee in question, to emphasize the importance of compliance with the CIP Visitor Control Program. Completed 7/25/2017
5) [redacted] Transmission Compliance will notify managers / supervisors that have direct reports with [redacted] CIP Substation unescorted badge access and instruct them on the NERC CIP visitor escort requirements. Completed 7/31/2017
6) The [redacted] Team ([redacted] shall conduct and complete their biennial review of Substation PSPs and report back any additional log book issues found. Completed 8/18/2017
7) [redacted] Ops Compliance shall produce and disseminate additional reinforcement on [redacted] CIP Visitor Control Program in the Q3 CIP Cyber Security awareness newsletter on proper escorting and logging responsibilities. Completed 9/14/2017
8) [redacted] and [redacted] Protection and Controls will verify through a review of before and after baseline configurations of devices in the substation that while the visitor was unescorted, they did not attempt to access and did not make any changes to any CIP systems while in the substation. 10/27/2017
9) [redacted] and [redacted] Protection and Controls will complete a CVA for all applicable CIP systems within the substation to confirm no unauthorized changes were made to devices within the substation. Complete by 10/27/2017
10) [redacted] Transmission Compliance will develop and have signage added to the [redacted] Medium substation PSPs providing reinforcement to on-site personnel on visitor escorting and logging responsibilities. Complete by 1/15/2018
11) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation. Complete by 1/31/2018

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

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

1/31/2018

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Baseline Config Review	10/27/2017	8) [redacted] and [redacted] Protection and Controls will verify through a review of before and after baseline configurations of devices in the substation that while the visitor was unescorted, they did not attempt to access and did not make any changes to any CIP systems while in the substation.	No
CVA Review	10/27/2017	9) [redacted] and [redacted] Protection and Controls will complete a CVA for all applicable CIP systems within the substation to confirm no unauthorized changes were made to devices within the substation.	No
Subs Signage	1/15/2018	10) [redacted] Transmission Compliance will develop and have signage added to the [redacted] Medium substation PSPs providing reinforcement to on-site personnel on visitor escorting and logging responsibilities.	Yes
Closure Package	1/31/2018	11) [redacted] Operations Compliance will complete a comprehensive review of all required evidence associated with this mitigation plan and prepare a summary closure packet for SERC review and settlement of this potential violation.	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 visitor logging issue at [redacted] Substation #1 posed a moderate potential risk, and did not pose a serious or substantial risk to the BES. Improperly logging of visitor access, which is a manual log book process at all Company PSPs, provides after-the-fact investigative documentation with little to no real-time impact to the BES. In this instance of improper logging at [redacted] Substation #1, proper escorting in accordance with CIP-006-6 R2.1 took place, and only the manual visitor log entries were mistakenly overlooked.

The subsequently discovered issues at [redacted] Substation #2 involving improper escorting of visitors within the PSP for an extended period of time has a higher degree of risk, in that, an unattended visitor within a Substation PSP could have resulted in adverse impact to the reliable operation of Transmission components at that Substation. The escort in this instance was authorized for unescorted physical access and had attended annual NERC CIP Cyber Security Training emphasizing the CIP-006-6 R2

Visitor Control Program and escort responsibilities. Although the escort was within the Substation yard while the visitor was within the PSP, leaving visitors unattended in the switch house was not in accordance with established policies and procedures.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

Provide detailed description of Actual Risk to Bulk Power System:

These issues posed a minimal actual risk and not a serious or substantial risk to the BES. As an investigative tool used to evaluate the situation at a PSP, Corporate Security has employed camera systems that in backup, emergency situations can be used to corroborate access details in an investigation. During the investigation of the Original Issue at [redacted] Substation #1, it was noted that the escort did properly exit the PSP with he visitors; however, the escort failed to annotate the exit times of the visitors in the manual visitor log book at that time. Upon discovery on 3/21/2017, surveillance footage and PACS [redacted] badge records (logs) confirmed the exit time of the escort and visitors from the PSP.

The subsequently discovered issues at [redacted] Substation #2 involving improper escorting of visitors within the PSP for an extended period of time, after investigation, was determined to also have a minimal potential risk, in that, the unattended visitor within the Substation PSP was a known contractor working for a vendor company with equipment in the Substation they were there to test. This contractor had entered [redacted] Substations previously before they became in scope of CIP V5. The escort in this instance was within the Substation yard while the visitor was within the PSP, and was periodically within the PSP to oversee and check on the contractor while performing testing. [redacted] Transmission does not feel that the lack of adherence to the Visitor Control Program is a pervasive issue at [redacted] 'Medium' Substations, and that targeted counseling/retraining with this individual, and re-emphasis through the [redacted] by the Transmission General Manager will help prevent future recurrence of these issues.

Additional Comments:

The [redacted] CIP Procedures Manual includes the following procedures addressing CIP-006-6 R2:
[redacted] Visitor Control Program, Section 4.1, part 4.1.1, page 2:
Continuous Escort of Visitors:
Any personnel not authorized for unescorted physical access to a specific CIP PSP through an approved Company Access Management Application (AMA) shall be considered a Visitor and shall be continuously escorted until unescorted physical access is appropriately authorized. For situations where an individual is appropriately authorized while inside a PSP, the individual must remain escorted until they have been properly signed out in the visitor access log, exit the PSP and then re-enter the PSP using his/her own credentials.

Only Authorized Users to a specific CIP PSP can act as an Escort for Visitors to that PSP. When escorting a Visitor, Authorized Users shall meet all Visitors at a PSP access point and maintain line-of-sight observation of Visitors at all times within a CIP PSP.

[redacted] Visitor Control Program, Section 4.1, part 4.1.2, page 3:
Logging of Visitor Access:
All Visitor access to a CIP PSP shall be logged via automated or manual means upon initial entry and final exit of a PSP access point, per day or shift. Where automated logging is not available, a manual visitor log shall be used.

The Authorized User(s) providing escort functions for a Visitor is responsible for ensuring all Visitor access to a CIP PSP is properly logged, to include date and time of the Visitor's initial entry into and final exit from the PSP, the Visitor's full first and last name, the reason for the visit, and the full first and last name of an individual point of contact responsible for the Visitor.

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)

VIEW MITIGATION PLAN CLOSURE: CIP-006-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEGEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 4/18/2019

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R2.	SERC2017-402868	SERC2017018441

Date of completion of the Mitigation Plan:

[redacted]

In Person [redacted] Retraining

Milestone Completed (Due: 10/13/2017 and Completed 10/10/2017)
Attachments (0)

3) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] with authorized unescorted physical access to the [redacted] The refresher training will be completed by 10/10/2017. [redacted]

In Person Facilities Retraining

Milestone Completed (Due: 10/20/2017 and Completed 10/12/2017)
Attachments (0)

4) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] rporate Facilities and personnel working for the contract [redacted] ng vendor with authorized unescorted physical access to the [redacted]. The refresher training will be completed by 10/20/2017.

Closure Package

Milestone Completed (Due: 10/27/2017 and Completed 10/16/2017)
Attachments (0)

5) [redacted] Operations Compliance shall produce a comprehensive closure package. 10/27/2017

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities: SERC2017-402868
1) [redacted] Ops Compliance and each [redacted] and [redacted] business unit shall perform an extent-of-condition review of a random sample of [redacted] PSP visitor log books to determine if any additional log book issues exist. (Completed 07/28/2017, prior to filing the self report)
2) [redacted] Ops Compliance shall disseminate additional reinforcement on [redacted] in the CIP quarterly awareness newsletter on proper escorting and logging responsibilities. (Completed 9/30/2017, prior to filing the self report)
3) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in the [redacted] with authorized unescorted physical access to the [redacted]. (Due 10/13/2017, Completed 10/10/2017)
4) [redacted] Transmission Compliance shall coordinate in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] Corporate Facilities and personnel working for the contract cleaning vendor with authorized unescorted physical access to the [redacted]. (Due 10/20/2017, Completed 10/12/2017)
5) [redacted] Operations Compliance shall produce a comprehensive closure package. (Due 10//27/2017, Completed 10/16/2017)
Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of Mitigating Activities: SERC2018-402982
1) [redacted] Ops Compliance and [redacted] Corporate Facilities shall perform an extent-of-condition review to determine if any other [redacted] Corporate Facilities employees escorted any contractors into a PSP to perform fire alarm testing on the evening of 12/19/2017 to ensure all visitors, if any, were properly logged in PSP visitor log books. (Completed 2/8/2018, prior to filing the self-report).
2) The [redacted] Corporate Operations & Maintenance Team Leader shall administer required in-person refresher training on CIP visitor control with the [redacted] facility operator that was responsible for escorting the contractor, covering visitor log book requirements and escort responsibilities when escorting visitors within a PSP. (Completed 2/15/2018, prior to filing the self-report)..
3) [redacted] Operations Compliance shall conduct in-person retraining on CIP visitor control responsibilities for personnel working in [redacted] Corporate Facilities. (Due 3/14/2018, Completed 2/21/2018).
4) [redacted] Operations Compliance shall produce a comprehensive closure package. (Due 3/28/2018, Completed 2/23/2018).
Details to Prevent Recurrence: Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

Description of the information provided to SERC for their evaluation *

[redacted] Closure Packet
Milestone 1:
[redacted] Demonstrates the extent-of-condition review of randomly sampled [redacted] PSP

visitor log books. The "PSPName" column identifies the PSPs visitor log books that were randomly sampled and "Issue in Log?" column indicates if there is a problem with the completion of the visitor log book. Row 51 is the line identifying an issue with the [redacted] visitor log book.

Milestone 2:

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[redacted] Demonstrates [redacted] (CIP-004-6 R1) disseminated to all Company personnel with CIP access on September 14th, 2017 reinforcing CIP Access Management requirements (Section: CIP Visitor Control) highlights the responsibilities of escorts to keep visitors in their line-of-sight, and verifying all required fields in the visitor log book are completed.

Milestone 3:

[redacted] Visitor Management presentation that was presented in-person by representatives from [redacted] Transmission Compliance to [redacted] personnel with authorized unescorted physical access to the [redacted]

[redacted] List o[redacted] personnel that attended the in-persor[redacted] visitor management responsibilities retraining conducted on 8/2/2017, 8/9/2017, 8/15/2017, 8/16/2017, 8/30/2017, 9/6/2017, 9/28/2017, and 10/10/2017.

Milestone 4:

[redacted] Visitor Management presentation that was presented in-person by representatives from [redacted] Transmission Compliance to the [redacted] corporate facilities personnel that have a business need for escorted or unescorted physical access to the [redacted]

[redacted] List of [redacted] corporate facilities personnel that attended the in-person visitor management responsibilities retraining conducted on 10/10/2017 and 10/12/2017.

[redacted] (Scope Expansion) [redacted] Closure Packet

Milestone 1:

[redacted]: Provides the report from the access management application ([redacted]) demonstrating that the contractor escort in issue #1 had his unescorted physical access to CIP PSPs revoked and removed (highlighted in yellow) on 6/8/2018.

Milestone 2:

[redacted]: Provides the PowerPoint presentation for issue #1 and issue #2 used to retrain the contractor serving as escort ([redacted]) and the [redacted] employee serving as an escor[redacted]) on the requirements for visitor control. The Visitor Control PowerPoint presentation is used as evidence for MS2 and MS5.

[redacted]: Provides evidence for issue #1 of a meeting on 7/9/2018 where the contractor serving as the escort [redacted] was retrained on the requirements for visitor control using the Visitor Control Presentation.

Milestone 3:

[redacted]: Provides evidence for issue #3 of the individual counseling meeting on 6/25/2018 with the security officer that did not verify the employee's unescorted physical access authorization to the PSP and opened the door for the employee returning from military leave.

Milestone 4:

[redacted] Provides evidence for issue #3 that all the security officers at the [redacted] facility as of 7/28/2018 were retrained on proper protocol for verifying an individual's authorized unescorted physical access to a PSP.

Milestone 5:

[redacted] Provides evidence for issue #2 of a meeting on 7/31/2018 where the [redacted] employee serving as the escort [redacted] was retrained on the requirements for visitor control using the Visitor Control Presentation.

Milestone 6:

[redacted]: Provides evidence for issue #4 where the contract employee requested and received appropriate access (highlighted in yellow) to the EMS [redacted] PSP and other EMS CIP datacenters in [redacted] based on his business need for access and to avoid escorting issues going forward.

Milestone 7:

[redacted]: Provides evidence of the EMS monthly baseline review showing that all system changes were accounted for with existing change management cases and therefore nothing was added or removed from the system while the Contract Employee was in the computer room, unescorted. The Installed Software Drift tab shows where any software changes to the systems all had an associated change record documenting the change. The Listening Network Ports Drift tab shows that all port drift is justified by whitelisting. The Operating System Drift tab shows that there was no associated OS drift detected. The Patches Drift ([redacted]) tab shows that all drift was covered by existing Change Management records. The Patches Drift [redacted] demonstrated that all [redacted] patch drift was covered by an existing Change Management record.

Milestone 8:

[redacted]: Provides evidence of the subject matter expert evaluation of the existing vulnerabilities on the system. A log review was performed after the incident and shows that no one logged into any systems (locally or remotely) while the contractor was unescorted at the site (see [redacted] below)
[redacted] Shows evidence of the logs produced by the vulnerability scan portion of the CVA. All vulnerabilities shown on the report are being addressed by EMS as part of their regular port scan and CVA remediation process. No new or additional vulnerabilities were detected.
[redacted] Shows evidence of the logs produced by the hosts within the PSP examined in the CVA. There was not any unusual or unexpected activity logged and no one logged into any system within the PSP during the time in which the unescorted visitor was inside the PSP.

Milestone 9:

[redacted] Shows evidence of the training delivered to members of the [redacted] Technology Organization team, where the visitor escort issue occurred. All team members were required to attend the visitor and escort training provided by [redacted] Technology Organization Compliance group personnel. The one member of the team invited who did not attend does not have unescorted Physical Access to any CIP PSPs and therefore, cannot escort visitors into a PSP.

Milestone 10:

[redacted] Provides three screenshots from the [redacted] Learning Management System (LMS) ([redacted]) showing the format of the NERC CIP Visitor Control video.
[redacted]: Provides the training voice script used to produce the NERC CIP Visitor Control video in the [redacted] LMS [redacted] to retrain personnel across [redacted] authorized for unescorted physical access to a CIP PSP on visitor control responsibilities.
[redacted]: Provides the list of personnel with authorized unescorted physical access to a CIP PSP ([redacted]) as of 8/20/2018 and verification that they completed the required Visitor Control training course or had their authorized unescorted physical access revoked. The Audience tab shows the list of personnel with authorized unescorted physical access to a CIP PSP. The LMS tab demonstrates an export direc ly from the [redacted] showing confirmation that the listed personnel in column A (REQUESTOR_NAME) across [redacted] with authorized unescorted physical access to a CIP PSP, completed "Attended" the retraining on CIP visitor control responsibilities as of 11/20/2018 as demonstrated in column C (Completed Training "Attended"). There were [redacted] individuals (starting on row [redacted] that were in the training audience as of 8/20/2018 for having unescorted physical access to a PSP at that time, but that did not complete the retraining by 11/20/2018. Column C (Reason for not completing the Training) explains the reason the individual did not attend the training – which included several terminations or retirements of personnel; for those individuals marked as "Revoked" who did not complete the retraining by the 11/20/2018 deadline, all of their unescorted physical access was revoked and removed until they complete the training, at which time they can re-request physical access to a PSP.

[redacted] CIP-006-6 R2.2 Closure Packet

Milestone 1:

[redacted]: Shows an email from the [redacted] Corporate Facilities Operations & Maintenance Team Lead that a review was completed on 2/8/2018 to verify that no other [redacted] Corporate Facilities employees escorted any contractors/visitors into a PSP to perform fire alarm testing on 12/19/2017.

Milestone 2:

[redacted]: Demonstrates that the [redacted] Corporate Facilities Operations & Maintenance Team Lead presented the CIP Visitor Control Refresher training material on 2/12/2018 to the individual [redacted] employee that was responsible for the visitor log book error.

[redacted] Provides the refresher training material on visitor control that was used to retrain the individual [redacted] employee that was the responsible for the visitor log book error.

Milestone 3:

[redacted]: Provides a list of the [redacted] Corporate Facilities personnel that were retrained on 2/21/2018 on the visitor control program, including an emphasis on accurately completing the visitor log book.

[redacted] Provides the training presentation used to retrain employees in [redacted] Corporate Facilities on 2/21/2018 on the visitor control program, including accurately completing the visitor log book.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.

Attachment 8

Record documents for the violation of CIP-007-6 R1

8a. The Entities' Self-Report (SERC2016016492)

8b. The Entities' Certification of Mitigation Plan Completion submitted January 19, 2017

VIEW SELF-REPORT: CIP-007-6 R1. (COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

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]
Applicable Requirement:	[redacted]
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:	7/27/2016
Beginning Date of Possible Violation:	7/1/2016
End or Expected End Date of Possible Violation:	8/2/2016
Is the violation still occurring?	No

Provide detailed description and cause of Possible Violation:

On 7/27/2016 [redacted] IT discovered a potential violation of CIP-007-6 R1.1 while performing cyber-security controls verification during the July 2016 Security Patch deployment. The [redacted] system (EACMS associated with Medium Impact BES Cyber Systems) had two ports, [redacted] and [redacted] opened which were not documented on the [redacted] Hosts ports and services whitelist. It was determined, prior to the commissioning of these Cyber Assets on July 1, 2016, the [redacted] service and the associated ports [redacted] and [redacted] were not required, and should be disabled. However, prior to commissioning on July 1, 2016, the [redacted] service was not disabled on the device until August 2, 2016 after discovery on July 27, 2016.

This potential issue is considered a failure to follow [redacted] NERC CIP procedure [redacted]. [redacted] instructs:
1) Ensure that all listening ports and services on the CIP Cyber System are either on the recorded whitelist for the CIP Cyber System or are covered under an associated TFE.
2) If discrepancies are found, do one of the following before commissioning:
- Disable the ports that are not found on the Ports and Services whitelist
- Create a new Ports and Services whitelist and update the baseline configuration for the CIP Cyber System.
- Update the TFE associated with this CIP Cyber System

Are Mitigating Activities in progress or completed? Yes

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

If Yes, Provide description of Mitiga ing Activities:

1) [redacted] IT will disable the [redacted] service on the device. Completed 8/2/2016
2) [redacted] IT will perform a review of all [redacted] CIP Cyber System baseline documentation and verify those ports and services documented in the baselines are the only ones enabled. (Due 11/18/2016)
3) Conduct a review session of the applicable [redacted] IT Work Practices addressing CIP-007-6 R1.1 and retrain department personnel on confirming only logical network accessible ports which are needed are enabled. (Due 12/9/2016)
4) Require department personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedure going forward. (Due 12/9/2016)

Provide details to prevent recurrence:

Successful completion of the above mitigation plan milestones will prevent future recurrence of this issue.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

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

12/9/2016

MITIGATING ACTIVITIES

Title	Due Date	Description	Prevents Recurrence
Disable Service	8/2/2016	[redacted] IT will disable the [redacted] service on the device.	No
Determine Extent of Condition in CIP Domain	11/18/2016	[redacted] IT will perform a review of all [redacted] CIP Cyber System baseline documentation and verify those ports and services documented in the baselines are the only ones enabled.	No
Retrain Dept Pesonnel	12/9/2016	Conduct a review session of the applicable [redacted] IT Work Practices addressing CIP-007-6 R1.1 and retrain department personnel on confirming only logical network accessible ports which are needed are enabled.	Yes
Attest to Abide by Procedures	12/9/2016	Require department personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedure going forward.	Yes

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]unknown [redacted] associated with this issue was not required, failure to follow documented processes to disable those ports and services led to additional services being enabled.

Provide detailed description of Actual Risk to Bulk Power System:

[redacted]red prior to [redacted]) is not Internet facing and is these Cyber Assets are behind layers of security within a dedicated protected CIP domain, the potential vulnerabilities that could possibly be exploited by this service running is very minimal. This potential issue is considered to be a result of a human performance error to follow documented procedures and will be addressed through retraining.

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)

VIEW MITIGATION PLAN CLOSURE: CIP-007-6 (MITIGATION PLAN CLOSURE COMPLETED)

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

This item was signed by [redacted] on 1/19/2017

MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for SERC to verify completion of the Mitigation Plan. SERC may request such additional data or information and conduct follow-up assessments, on-site or other Spot Checking, or Compliance Audits as it deems necessary to verify that all required actions in the Mitigation Plan have been completed and the Registered Entity is in compliance with the subject Reliability Standard. (CMEP Section 6.6) Data or information submitted may become part of a public record upon final disposition of the possible violation, therefore any confidential information contained therein should be marked as such in accordance with the provisions of Section 1500 of the NERC Rules of Procedure.

Name of Registered Entity submitting certification:

[redacted]

Name of Standard of mitigation violation(s):

[redacted]

Requirement	Tracking Number	NERC Violation ID
R1.	SERC2016-402526	SERC2016016492

Date of completion of the Mitigation Plan:

[redacted]

Disable Service

Milestone Completed (Due: 8/2/2016 and Completed 8/2/2016)
Attachments (0)

[redacted] IT will disable he[redacted] service on the device.

Determine Extent of Condition in CIP Domain

Milestone Completed (Due: 11/18/2016 and Completed 11/18/2016)
Attachments (0)

[redacted] IT will perform a review of all[redacted]P Cyber System baseline documentation and verify those ports and services documented in the baselines are the only ones enabled.

Retrain Dept Pesonnel

Milestone Completed (Due: 12/9/2016 and Completed 12/6/2016)
Attachments (0)

[redacted]duct a review session of the ap[redacted] IT Work Practices addressing CIP-007-6 R1.1 and retrain department personnel on confirming only logical network accessible ports which are needed are enabled.

Attest to Abide by Procedures

Milestone Completed (Due: 12/9/2016 and Completed 12/7/2016)
Attachments (0)

[redacted]uire department personnel to s[redacted]ation attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedure going forward.

Summary of all actions described in Part D of the relevant mitigation plan:

Description of Mitigating Activities:
1)[redacted] IT will disable the[redacted]service on the device.
2)[redacted] IT will perform a review of all[redacted] CIP Cyber System baseline documentation and verify those ports and services documented in the baselines are the only ones enabled.
3) Conduct a review session of the applicable[redacted] IT Work Practices addressing CIP-007-6 R1.1 and retrain department personnel on confirming only logical network accessible ports which are needed are enabled.
4) Require department personnel to sign documentation attesting that they have reviewed and understand the applicable procedural steps, and agree to abide by the procedure going forward.

Description of the information provided to SERC for their evaluation *

Milestone 1:
[redacted]; Page 1 provides evidence demonstrating the authorization for disabling the[redacted] Service, which was completed on 8/2/2016. Page 2, provides a screen shot from the device showing the service was disabled on 8/2/2016.

Milestone 2:
The following documentation demonstrates the results of the review performed by[redacted]-IT of al[redacted] cyber system ports and services to ensure all enabled network accessible ports and services accurately reflected each device's applicable baseline documentation. The purpose of the reviews was to verify those ports and services documented as authorized in the applicable device baseline documentation was accurate and reflected the current state of network accessible ports and services. The following[redacted]-IT managed cyber systems were reviewed:
[redacted] / [redacted] / [redacted] Logger - EACMS used to perform CIP-007-6 R4 Security Event Monitoring of Substation devices. There are[redacted] physical

[redacted] servers, [redacted] servers and [redacted] Logger appliances managed by [redacted]-IT.
- [redacted] – EACMS used to manage each of the [redacted] Medium Substation ESP firewalls. There is [redacted] virtual CMS server managed by [redacted]-IT.
- [redacted] - EACMS used to implement [redacted] authentication on cyber assets within the [redacted] Domain. There are [redacted] appliances managed by [redacted]-IT.
- [redacted] - EACMS used to house the [redacted] cyber assets; there are [redacted] physical servers managed by [redacted]-IT.
- [redacted] Domain Controller - EACMS domain controller for the [redacted] domain. There are [redacted] servers managed by [redacted]-IT.
- [redacted] - EACMS Intermediate System used for Interactive Remote Access into Substation ESPs. There are [redacted] servers managed by [redacted]-IT.

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

[redacted] provides a ports and services review completed on 11/18/2016 for the following [redacted]-IT managed cyber systems:
- [redacted] – the following servers were reviewed; [redacted]
- [redacted] - the following server was reviewed [redacted].
- [redacted] Domain Controller - the following servers were reviewed [redacted]
- [redacted] - the following servers were reviewed; [redacted]

Pages 1-29 provide the ports and services review, pages 30-41 provide the port and services whitelists for the specific cyber systems. Pages 42 – 44 provide the dependent whitelist for the [redacted] OS.

[redacted], pages 1-2, provides the ports and services review for [redacted] completed on 11/14/2016, page 3 provides the ports and services whitelist for the [redacted] servers.

[redacted] pages 1-2, provides the ports and services review for the [redacted] appliances completed on 10/31/2016, page 3 provides the ports and services whitelist for the [redacted].

[redacted], pages 1-2, provides the ports and services review for the [redacted] appliances completed on 10/24/2016, page 3 provides the ports and services whitelist for [redacted]

[redacted] pages 1-2, provides the ports and services review for the [redacted] servers completed on 11/1/2016, page 3 provides the ports and services whitelist for [redacted]

Milestone 3:
[redacted] Presentation used to retrain [redacted] IT employees and managers on the Ports and Services / Whitelist Program. The training sessions were scheduled based on specific departments within IT, and the last training session was completed on 12/6/2016. See CIP-007 R1.1 [redacted] for the list of attendees to these training sessions.

[redacted] provides a list of attendees that participated in the [redacted] CIP Information Protection Program refresher training, and depicts the date, department, and list of attendees for each session.

[redacted] Cyber System Management Procedure reviewed in each of the training sessions. Section [redacted] "Commissioning Stage", steps 1-3 requires ports which have been determined to be needed are listed on a whitelist for the CIP Cyber System. If they are not listed the then the ports should be disabled or the whitelist and baseline configuration documentation should be updated.

Milestone 4:
[redacted] provides a sample of the attestation completed by each attendee of the above training sessions attesting that they have reviewed and understand the applicable governance procedures and business unit work practice procedural steps referenced in milestone 3, and that they agree to abide by those procedures going forward.

I certify that the Mitigation Plan for the above-named violation has been completed on the date shown above. In doing so, I certify that all required Mitigation Plan actions described in Part D of the relevant Mitigation Plan have been completed, compliance has been restored, the above-named entity is currently compliant with all of the requirements of the referenced standard, and that all information submitted is complete, true and correct to the best of my knowledge.