

April 30, 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]**  
**FERC Docket No. NP19-\_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty<sup>1</sup> regarding [REDACTED] (The Entity), NERC Registry ID# [REDACTED]<sup>2</sup> with information and details regarding the nature and resolution of the violations<sup>3</sup> discussed in detail in the Settlement Agreement attached hereto (Attachment A), 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)).<sup>4</sup>

NERC is filing this Notice of Penalty with the Commission because the Florida Reliability Coordinating Council (FRCC) and The Entity have entered into a Settlement Agreement to resolve all outstanding issues arising from FRCC's determination and findings of the violations of CIP-004-6 R4, CIP-004-6 R5, CIP-007-6 R1, CIP-007-6 R2, CIP-007-6 R4, CIP-007-6 R5, CIP-010-2 R1, CIP-010-2 R3, and CIP-011-2 R1. According to the Settlement Agreement, The Entity neither admits nor denies the violations, but has agreed to the assessed penalty of three hundred one thousand dollars (\$301,000), in addition to other remedies and

---

<sup>1</sup> 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).

<sup>2</sup> [REDACTED] was included on the NERC Compliance Registry as a [REDACTED]

<sup>3</sup> 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.

<sup>4</sup> See 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

**3353 Peachtree Road NE**  
**Suite 600, North Tower**  
**Atlanta, GA 30326**  
**404-446-2560 | www.nerc.com**

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 2

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

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 The Entity and FRCC. 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. Further information on the subject violations is set forth in the Settlement Agreement and herein.

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 3

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

<b>Violation(s) Determined and Discovery Method</b>								
*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
FRCC2017017834	CIP-004-6	R4	Medium/ Severe		SR [REDACTED]	3/17/2017 – 7/31/2017	Moderate	\$301,000
FRCC2017017370	CIP-004-6	R4	Medium/ Severe		SR [REDACTED]	10/1/2016 – 11/20/2017	Moderate	
FRCC2017017454	CIP-004-6	R5	Medium/ Lower		SR [REDACTED]	7/1/2016 – 5/8/2017	Minimal	
FRCC2017017869	CIP-007-6	R1	Medium/ Severe		SR [REDACTED]	7/1/2016 – 3/30/2018	Minimal	
FRCC2017017375	CIP-007-6	R2	Medium/ Moderate		SR [REDACTED]	7/1/2016 – 7/13/2018	Serious	
FRCC2017017833	CIP-007-6	R4	Medium/ Severe		SR [REDACTED]	7/1/2016 – 4/18/2018	Moderate	
FRCC2017017857	CIP-007-6	R5	Medium/ Severe		SR [REDACTED]	7/1/2016 – 1/15/2018	Moderate	
FRCC2017017376	CIP-010-2	R1	Medium/ High		SR [REDACTED]	7/1/2016 – 11/15/2017	Moderate	
FRCC2017017835	CIP-010-2	R3	Medium/ Severe		SR [REDACTED]	12/1/2016 – 6/27/2017	Moderate	
FRCC2017017696	CIP-011-2	R1	Medium/ Severe		SR [REDACTED]	7/1/2016 – 1/10/2018	Moderate	

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 4

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

#### FACTS COMMON TO VIOLATIONS

The Entity discovered these violations in [REDACTED] in preparation for a CIP Compliance Audit. All 10 violations were submitted as Self-Reports, with the majority of the Self-Reports submitted after The Entity received the audit notification letter.

Historically, The Entity has been compliant with the CIP Standards; however, during the transition from CIP Version 3 to CIP Version 5, The Entity had a breakdown in compliance with the CIP Standards. This breakdown and the following violations can be attributed to insufficient management oversight, a lack of internal controls, and poorly documented and poorly followed processes and procedures.

#### CIP-004-6 R4

FRCC determined that The Entity failed to adhere to the requirements of CIP-004-6 R4 in two instances:

1. In the first instance, The Entity failed to authorize electronic access based on need for electronic access for three individuals as required by CIP-004-6 R4 (Part 4.1). Attachment 2 includes additional facts regarding the violation.

The root cause for this violation was the failure to follow the procedure, lack of internal controls, and insufficient management oversight during the authorization process.

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 3a.

The Entity certified that it had completed all mitigation activities. FRCC verified that The Entity had completed all mitigation activities as of September 10, 2018. Attachments 3b and 3c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

2. In the second instance, FRCC determined that The Entity failed to verify, at least once each calendar quarter, that individuals with active electronic access or unescorted physical access had authorization records as required by CIP-004-6 R4, Part 4.2. The causes for this violation were an incorrect interpretation of the procedure by the Subject Matter Expert (SME), lack of internal controls, and insufficient management oversight during the control verification process.



NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 5

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

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 4a.

The Entity certified that it had completed all mitigation activities. FRCC verified that The Entity had completed all mitigation activities as of September 10, 2018. Attachments 4b and 4c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

#### CIP-004-6 R5

FRCC determined that The Entity did not revoke an individual's access to the designated storage locations for BES Cyber System Information (BCSI), whether physical or electronic, by the end of the next calendar day following the effective date of the termination action as required by CIP-004-6 R5, Part 5.3. The contributing causes for this violation were the failure to follow The Entity's process for personnel termination, a lack of internal controls, and insufficient management oversight during the revocation process.

FRCC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Attachment 2 includes the facts regarding the violation that FRCC considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 5a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 10, 2018. Attachments 5b and 5c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

#### CIP-007-6-R1

FRCC determined that The Entity failed to properly determine logical network accessible port ranges or services needed to handle dynamic ports on seven Electronic Access Control or Monitoring (EACM) Cyber

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 6

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

Assets. The causes for this violation were the incorrect interpretation of the procedure by the SME, inadequate internal controls, no documented testing requirements, and insufficient management oversight during the ports and services authentication process.

FRCC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Attachment 2 includes the facts regarding the violation that FRCC considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 6a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 24, 2018. Attachments 6b and 6c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

#### CIP-007-6 R2

FRCC determined that The Entity failed to:

1. follow its patch management process for tracking cyber security patches for applicable Cyber Assets as required by CIP-007-6 R2, Part 2.1;
2. evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 at least once every 35 days as required by CIP-007-6 R2, Part 2.2; and
3. take one of the following actions within 35 calendar days of the evaluation completion: apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan as required by CIP-007-6 R2, Part 2.3.

The causes for this violation were a failure to follow The Entity's process, poorly documented internal controls and lack of internal controls during the verification and periodic review.

FRCC determined that this violation posed a serious risk to the reliability of the bulk power system (BPS). Attachment 2 includes the facts regarding the violation that FRCC considered in its risk assessment.

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigation activities The Entity took to address this violation. A copy of the Mitigation Plan and the Mitigation Plan Extension Request are included as Attachments 7a and 7b.

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 7

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

The Entity certified that it had completed all mitigation activities. FRCC verified that The Entity had completed all mitigation activities as of September 27, 2018. Attachments 7c and 7d provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

CIP-007-6 R4

FRCC determined that The Entity failed to log the minimum required events at the BES Cyber System or the Cyber Asset level capability. Specifically, The Entity failed to log events related to successful login attempts, detected failed access attempts and failed login attempts on 17 BES Cyber Asset (BCA) workstations and five Physical Access Control Systems (PACS). The causes for this violation were the SME's failure to follow the process, inadequate internal controls, no testing requirement, no periodic review, and insufficient management oversight.

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan and the Mitigation Plan Extension request are included as Attachments 8a and 8b.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 13, 2018. Attachments 8c and 8d provide specific information on FRCC's verification of The Entity's completion of the activities.

CIP-007-6 R5

FRCC determined that The Entity failed to limit unsuccessful authentication attempts, alert for unsuccessful authentication attempts, or file a Technical Feasibility Exception. Specifically, The Entity failed to implement controls to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts on seven Electronic Access Control or Monitoring (EACM) devices as required by CIP-007-6 R5, Part 5.7. The causes for this violation were due to the SME's incorrect interpretation of the procedure, lack of internal controls, no documentation of testing requirements, and insufficient management oversight during the access controls process.

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

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 8

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 9a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 13, 2018. Attachments 9b and 9c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

CIP-010-2 R1

FRCC determined that The Entity failed to develop baseline configurations for five Intrusion Protection System (IPS) Cyber Assets and failed to document changes from the existing baselines on seven Security Information and Event Management devices (SIEMs). The causes for this issue were an incomplete process and a lack of internal controls to ensure authorization of changes and updates to baselines occurred.

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 10a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 11, 2018. Attachments 10b and 10c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

CIP-010-2 R3

FRCC determined that The Entity added two switches to manage network isolation of the production environment as PCAs without performing a vulnerability assessment as required by CIP-010-2 R3 Part 3.3.

The causes for this violation were an incomplete documented procedure, lack of internal controls, and insufficient management oversight during the configuration change management process.

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 9

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

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 11a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 24, 2018. Attachments 11b and 11c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

#### CIP-011-2 R1

FRCC determined that The Entity failed to implement one or more documented information protection program(s) that would identify all storage locations that included BCSI as required by CIP-011-2 R1.1. The causes for this violation were the SME's incorrect interpretation of the Standard, no documented procedure, lack of internal controls, and insufficient management oversight during the BCSI identification process.

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

The Entity submitted its Mitigation Plan to address the referenced violation. Attachment 2 includes a description of the mitigating activities The Entity took to address this violation. A copy of the Mitigation Plan is included as Attachment 12a.

The Entity certified that it had completed all mitigating activities. FRCC verified that The Entity had completed all mitigating activities as of September 12, 2018. Attachments 11b and 11c provide specific information on The Entity's certification and FRCC's verification of the completion of the mitigating activities.

#### Regional Entity's Basis for Penalty

According to the Settlement Agreement, FRCC has assessed a penalty of three hundred one thousand dollars (\$301,000) for the referenced violations. In reaching this determination, considered the following factors:

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 10

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

1. FRCC considered the instant violations as repeat noncompliance with the subject NERC Reliability Standards. FRCC considered The Entity's compliance history with CIP-007-1 R2, CIP-007-3a R2, and CIP-007-6 R2 as an aggravating factor in the penalty determination;<sup>5</sup>
2. The Entity had an internal compliance program at the time of the violation that operated successfully until the complex challenges of the transition to CIP Version 5, for which FRCC awarded a small mitigating credit, as discussed in Attachment 1;
3. The Entity self-reported three violations before the date that FRCC sent the audit notification to The Entity, for which FRCC awarded mitigating credit. FRCC did not award The Entity credit for submitting the seven other self-reports because The Entity submitted them after FRCC sent an audit notification letter;
4. The Entity was cooperative, especially on the senior-management level, throughout the compliance enforcement process, for which FRCC awarded small mitigating credit;
5. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

After consideration of the above factors, FRCC determined that, in this instance, the penalty amount of three hundred one thousand dollars (\$301,000) 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<sup>6</sup>**

#### **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,<sup>7</sup> the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on March 20, 2019 and approved the resolution between FRCC and The Entity. 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.

---

<sup>5</sup> The Entity's relevant prior noncompliance with CIP-007-1 R2, CIP-007-3a R2, and CIP-007-6 R2 includes: [REDACTED]

<sup>6</sup> See 18 C.F.R. § 39.7(d)(4).

<sup>7</sup> *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).

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 11

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

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of three hundred one thousand dollars (\$301,000) is appropriate for the 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 an entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publicly, 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.<sup>8</sup>

- a. 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

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.<sup>9</sup> The redacted information includes details that could lead to identification of The

---

<sup>8</sup> 18 C.F.R. § 388.113(e)(1).

<sup>9</sup> NERC has previously filed dispositions of CIP violations on a nonpublic basis because of this regulation. To date, the Commission has directed public disclosure regarding the disposition of CIP violations in only a small number of cases. See Freedom of Information Act Appeal, FOIA No. FY18-75 (August 2, 2018); FOIA No. FY19-019 Determinations on Docket Nos. NP14-32 and NP14-41 (February 28, 2019). Based on the facts specific to 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.



NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 12

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

Entity, and information about the security of The Entity's systems and operations, such as specific processes, configurations, or tools The Entity uses to manage its cyber systems. As the Commission has previously recognized, information related to CIP violations and cyber security issues, including the identity of The Entity, 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."<sup>10</sup>

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of The Entity and any information that could lead to its identification.<sup>11</sup> Information that could lead to the identification of The Entity includes The Entity's name, its NERC Compliance Registry ID, and information regarding the size and characteristics of The Entity's operations.

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

b. 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

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 useful to a person planning an attack on The Entity's critical infrastructure. The incapacity or destruction of The Entity's 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 a specific cyber security issue and related vulnerabilities, as well as details concerning the types and configurations of

---

<sup>10</sup> *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).

<sup>11</sup> See the next section for a list of this information.

<sup>12</sup> See below for a list of this information.

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 13

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

The Entity's 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 Entity, 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 Entity's vendors and contractors.
3. The NERC Compliance Registry numbers of The Entity.
4. The registered functions and registration dates of The Entity.
5. The names of The Entity's facilities.
6. The names of The Entity's assets.
7. The names of The Entity's employees.
8. The names of departments that are unique to The Entity.
9. The sizes and scopes of The Entity's 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, April 30, 2019. Details about The Entity's operations, networks, and security should be treated and evaluated separately from its 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, April 30, 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 Entity to ensure sustainability of the improvements described in this Notice of Penalty; and
2. Remediation of any subsequent violations discovered through compliance monitoring by the Regions.

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

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 14

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

**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 FRCC and The Entity executed February 11, 2019, included as Attachment 1;
2. Details of the Violations, included as Attachment 2;
3. The Entity's Mitigation Plan designated as FRCCMIT013372 for CIP-004-6 R4 submitted November 9, 2017, included as Attachment 3a;
4. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted June 12, 2018, included as Attachment 3b;
5. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated September 10, 2018, included as Attachment 3c;
6. The Entity's Mitigation Plan designated as FRCCMIT013384 for CIP-004-6 R4 submitted November 16, 2017, included as Attachment 4a;
7. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted June 12, 2018, included as Attachment 4b;
8. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated September 10, 2018, included as Attachment 4c;
9. The Entity's Mitigation Plan designated as FRCCMIT013371 for CIP-004-6 R5 submitted November 9, 2017, included as Attachment 5a;
10. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R5 submitted June 12, 2018, included as Attachment 5b;
11. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R5 dated September 10, 2018, included as Attachment 5c;
12. The Entity's Mitigation Plan designated as FRCCMIT013376 for CIP-007-6 R1 submitted November 9, 2017, included as Attachment 6a;
13. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R1 submitted July 18, 2018, included as Attachment 6b;
14. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R1 dated September 24, 2018, included as Attachment 6c;
15. The Entity's Mitigation Plan designated as FRCCMIT013383 for CIP-007-6 R2 submitted November 16, 2017, included as Attachment 7a;
16. The Entity's Request for Mitigation Plan Extension for CIP-007-6 R2 submitted June 18, 2018, included as Attachment 7b;

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 15

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

17. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R2 submitted July 19, 2018, included as Attachment 7c;
18. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R2 dated September 27, 2018, included as Attachment 7d;
19. The Entity's Mitigation Plan designated as FRCCMIT013383 for CIP-007-6 R4 submitted November 9, 2017, included as Attachment 8a;
20. The Entity's Request for Mitigation Plan Extension for CIP-007-6 R4 submitted June 18, 2018, included as Attachment 8b;
21. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R4 submitted July 12, 2018, included as Attachment 8c;
22. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R4 dated September 13, 2018, included as Attachment 8d;
23. The Entity's Mitigation Plan designated as FRCCMIT013382 for CIP-007-6 R5 submitted November 16, 2017, included as Attachment 9a;
24. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R5 submitted July 18, 2018, included as Attachment 9b;
25. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R5 dated September 13, 2018, included as Attachment 9c;
26. The Entity's Mitigation Plan designated as FRCCMIT013374 for CIP-010-2 R1 submitted November 9, 2017, included as Attachment 10a;
27. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R1 submitted July 18, 2018, included as Attachment 10b;
28. FRCC's Verification of Mitigation Plan Completion for CIP-010-2 R1 dated September 11, 2018, included as Attachment 10c;
29. The Entity's Mitigation Plan designated as FRCCMIT013370 for CIP-010-2 R3 submitted November 9, 2017, included as Attachment 11a;
30. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R3 submitted June 12, 2018, included as Attachment 11b;
31. FRCC's Verification of Mitigation Plan Completion for CIP-010-2 R3 dated September 24, 2018, included as Attachment 11c;
32. The Entity's Mitigation Plan designated as FRCCMIT013373 for CIP-011-2 R1 submitted November 9, 2017, included as Attachment 12a;

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 16

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

33. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted June 12, 2018, included as Attachment 12b;
34. FRCC's Verification of Mitigation Plan Completion for CIP-011-2 R1 dated September 11, 2018, included as Attachment 12c.

NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 17

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

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

<p>*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.</p> <p>Stacy Dochoda* President and Chief Executive Officer Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 600 Tampa, Florida 33607-8410 (813) 207-7960 <a href="mailto:sdochoda@frcc.com">sdochoda@frcc.com</a></p> <p>John Odom* VP Compliance, Enforcement and Reliability Performance Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 600 Tampa, Florida 33607-8410 (813) 207-7985 <a href="mailto:jodom@frcc.com">jodom@frcc.com</a></p> <p>Andrew Williamson* Director of Enforcement, Risk Assessment &amp; Mitigation Florida Reliability Coordinating Council, Inc. 3000 Bayport Drive, Suite 600 Tampa, Florida 33607-8410 (813) 289-5647 <a href="mailto:awilliamson@frcc.com">awilliamson@frcc.com</a></p>	<p>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 <a href="mailto:edwin.kichline@nerc.net">edwin.kichline@nerc.net</a></p> <p>Emily Burgis Associate Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile <a href="mailto:Emily.Burgis@nerc.net">Emily.Burgis@nerc.net</a></p>
---	--

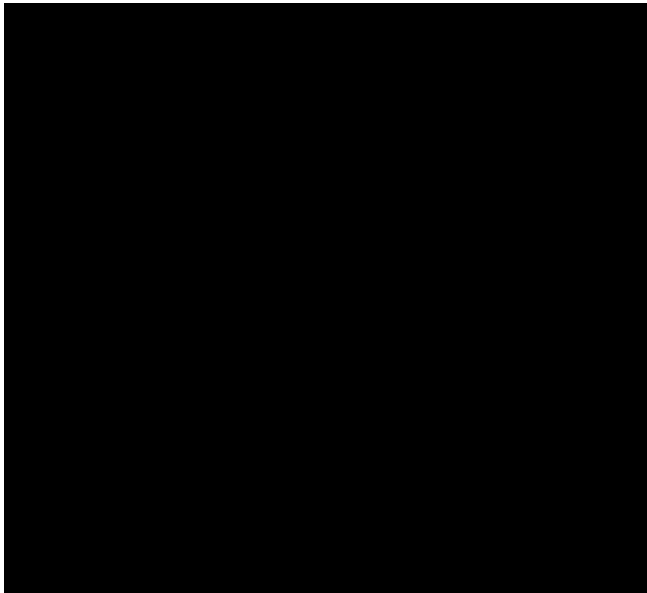
NERC Notice of Penalty

The Entity

April 30, 2019

Page 18

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

	
---	--



NERC Notice of Penalty  
The Entity  
April 30, 2019  
Page 19

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

**Conclusion**

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

Respectfully submitted,

*/s/ Emily Burgis*  
Edwin G. Kichline  
Senior Counsel and Director of  
Enforcement Oversight  
Emily Burgis  
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  
Emily.Burgis@nerc.net

cc:

  
FRCC

Attachments

Attachment 1

Settlement Agreement by and between  
FRCC and The Entity executed February 11, 2019



FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

### Settlement Agreement

██████████ ("the Entity") and Florida Reliability Coordinating Council, Inc. ("the Region") agree to the following:

1. The Entity neither admits nor denies the violations of NERC Reliability Standard as listed in Attachment A and has agreed to the proposed penalty of \$301,000 to be assessed to the Entity, in addition to mitigation actions undertaken to mitigate the instant alleged violations.
2. This Settlement Agreement is subject to approval or modification by the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC or Commission). Payment terms will be set forth in the invoice to be submitted by the Region after Commission approval of the instant Notice of Penalty.
3. The Entity has agreed to enter into this Settlement Agreement with the Region to avoid extended litigation with respect to the matters described or referred to herein, to avoid uncertainty, and to effectuate a complete and final resolution of the issues set forth herein. The Entity agrees that this Settlement Agreement is in the best interest of the parties and in the best interest of bulk-power system reliability.
4. The Entity has no additional statements.
5. The violations listed below and in Attachment A will be considered Alleged Violations that the Entity neither admits nor denies by NERC, the Region and the Federal Energy Regulatory Commission for all purposes and may be used as aggravating factors in accordance with the NERC Sanction Guidelines for determining appropriate monetary penalties or sanctions for future violations.

Issue Tracking #	FRCC Tracking #	Standard	Req.	Method of Discovery	Date Reported	Function Affected
FRCC 2017017834	FRCC2017	100936	CIP-004-6	R4.	Self-Report	██████████
FRCC 2017017370	FRCC2017	100921	CIP-004-6	R4.	Self-Report	██████████
FRCC 2017017454	FRCC2017	100924	CIP-004-6	R5.	Self-Report	██████████
FRCC 2017017869	FRCC2017	100939	CIP-007-6	R1.	Self-Report	██████████
FRCC 2017017375	FRCC2017	100923	CIP-007-6	R2.	Self-Report	██████████
FRCC 2017017833	FRCC2017	100935	CIP-007-6	R4.	Self-Report	██████████
FRCC 2017017857	FRCC2017	100938	CIP-007-6	R5.	Self-Report	██████████
FRCC 2017017376	FRCC2017	100922	CIP-010-2	R1.	Self-Report	██████████
FRCC 2017017835	FRCC2017	100937	CIP-010-2	R3.	Self-Report	██████████
FRCC 2017017696	FRCC2017	100929	CIP-011-2	R1.	Self-Report	██████████

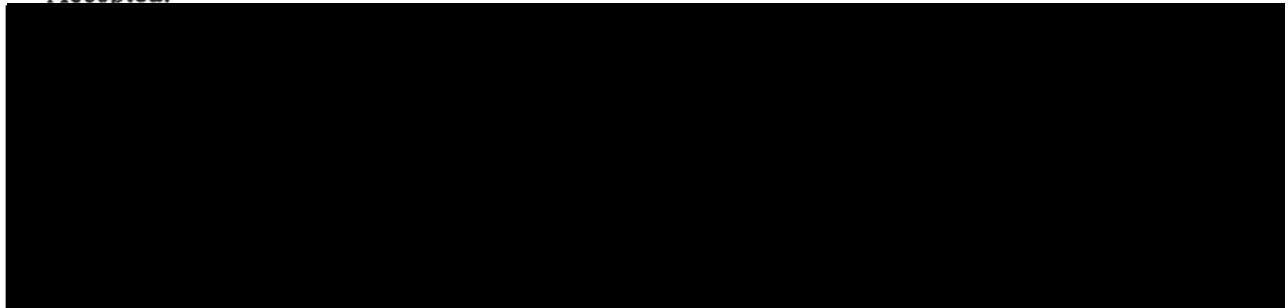
6. The Region has verified that the violations listed in Attachment A have been mitigated as described in Attachment A.



FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

7. The expedited disposition agreed to herein represents a full and final disposition of the violations listed in Attachment A, subject to approval or modification by NERC and FERC. The Entity waives its right to further hearings and appeal, unless and only to the extent that the Entity contends that any NERC or Commission action on this Settlement Agreement contains one or more material modifications to this Settlement Agreement.
8. In the event the Entity fails to comply with any of the stipulations, remedies, sanctions or additional terms, as set forth in this Settlement Agreement, the Region will initiate enforcement, penalty, or sanction actions against the Entity to the maximum extent allowed by the NERC Rules of Procedure, up to the maximum statutorily allowed penalty. Except as otherwise specified in this Settlement Agreement, the Entity shall retain all rights to defend against such enforcement actions, also according to the NERC Rules of Procedure.
9. Each of the undersigned warrants that he or she is an authorized representative of the entity designated, is authorized to bind such entity and accepts the Settlement Agreement on the entity's behalf.
10. The undersigned representative of each party affirms that he or she has read the Settlement Agreement, that all of the matters set forth in the Settlement Agreement are true and correct to the best of his or her knowledge, information and belief, and that he or she understands that the Settlement Agreement is entered into by such party in express reliance on those representations.

Accepted:





**John E Odom**



**Date**

Vice President, Compliance, Enforcement and Reliability Performance  
Florida Reliability Coordinating Council, Inc.

Attachment 2

FRCC's Details of the violations

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017834	CIP-004-6	R4., 4.1.	Medium	Severe	3/17/2017 (when the Entity failed to properly authorize access)	7/31/2017 (when the Entity corrected the current access group to include only authorized users and obtain authorization for required members)	Self-Report	1/30/2018	9/10/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █ the Entity submitted a Self-Report stating that, as a Balancing Authority, Distribution Provider, █, it had a violation of CIP-004-6 R4, Part 4.1.  The Entity failed to authorize electronic access for three (3) individuals. In three (3) instances, the Entity failed to authorize access based on need for electronic access as required by CIP-004-6 R4 (Part 4.1).  In the first instance, a network administrator was granted access to the Entity’s CIP Electronic Access Control or Monitoring (EACM) Cyber Assets associated with high impact BES Cyber Systems (BCS) without first receiving proper authorization.  In the second and third instances, two (2) individuals were granted access for the users' individual accounts without proper authorization, however their access to administrative accounts was properly authorized.  The extent of condition review identified one (1) additional individual without proper authorization in two (2) instances. The total number of individuals involved in the violation is four (4) authorized users with five (5) instances.  The root cause for this violation was the failure to follow the procedure, lack of internal controls, and insufficient management oversight during the authorization process.						
<b>Risk Assessment</b>			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  Specifically, the Entity’s failure to properly authorize individuals before granting access to BES Cyber Assets (BCAs) had the potential to affect the reliable operation of the BPS. By providing the opportunity for unauthorized personnel to access BCAs, the unauthorized access could compromise the integrity of the BCAs.  The risk was reduced because all individuals had valid Personnel Risk Assessments (PRAs) and were current with their CIP Cyber Security training.  No harm is known to have occurred.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) completed quarterly review; 2) corrected the current access group to include only authorized users and obtain authorization for required members and revoke access for users who do not require access or cannot be authorized in a timely manner; 3) updated procedure to state that all account access must be requested and approved, even if the account that belongs to user already approved under separate account and document quarterly review for authorization process; 4) updated controls to ensure that administrative accounts are limited for administration-only and user-only accounts are not allowed administrative privilege; 5) updated procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc.; 6) documented single verifiable reference sources used for authorization approval and ensured that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc.; 7) completed extent of condition review; 8) identified root cause for violation; and 9) completed training or certification of acknowledgement for SMEs for understanding of newly designed controls.						



NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017834	CIP-004-6	R4., 4.1.	Medium	Severe	3/17/2017 (when the Entity failed to properly authorize access)	7/31/2017 (when the Entity corrected the current access group to include only authorized users and obtain authorization for required members)	Self-Report	1/30/2018	9/10/2018
Other Factors			The Region reviewed the Entity's compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						



NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017370	CIP-004-6	R4., 4.2.	Medium	Severe	10/1/2016 (when the Entity failed to verify electronic or physical access)	11/30/2017 (when the Entity completed the verification of those individuals with active electronic access or unescorted physical access who had authorization records issues)	Self-Report	1/30/2018	09/10/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			<p>On ██████, the Entity submitted a Self-Report stating that, as a ██████ it was in violation of CIP-004-6 Requirement 4, Part 4.2.</p> <p>The Entity failed to verify, at least once each calendar quarter, that individuals with active electronic access or unescorted physical access have authorization records as required by CIP-004-6 R4, Part 4.2.</p> <p>Initially, the Entity self-reported from the effective date of the Standard, July 1, 2016, the Entity did not perform a quarterly verification for three (3) calendar quarters.</p> <p>During an extent of condition review, there were an additional two (2) calendar quarters where the Entity did not perform the quarterly review as required.</p> <p>The causes for this violation were an incorrect interpretation of the procedure by the Subject Matter Expert (SME), lack of internal controls, and insufficient management oversight during the control verification process.</p>						
<b>Risk Assessment</b>			<p>This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The Entity’s failure to verify the authorization of those individuals with active electronic or unescorted physical access could have allowed unauthorized access to high and medium impact Bulk Electric System Cyber Systems (BCS). The unauthorized access could have compromised the BCS, allowing them to affect the reliable operation of the BPS.</p> <p>The risk was reduced as the Entity was performing a review based on their version 3 process; however, they had not implemented the new version 5 process.</p> <p>No harm is known to have occurred.</p>						
<b>Mitigation</b>			<p>To mitigate this violation, the Entity:</p> <ol style="list-style-type: none"><li>1) corrected access issues after completion of quarterly authorization;</li><li>2) updated procedure to state that all accounts access must be requested and approved, even if the account belongs to user already approved under separate account;</li><li>3) updated controls to ensure that administrative accounts are limited for administration-only and user-only accounts are not allowed administrative privilege;</li><li>4) updated procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc.);</li><li>5) documented single verifiable reference sources used for authorization approval and ensured that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc.);</li><li>6) completed extent of condition review;</li><li>7) identified root cause for violation; and</li><li>8) completed training or certification of acknowledgement for SME for understanding of newly designed controls.</li></ol>						
<b>Other Factors</b>			<p>The Region reviewed the Entity’s compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations. In Addition, Self-Reporting credit was awarded for violations that were self-reported prior to the entity receiving the audit notification letter.</p>						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017454	CIP-004-6	R5., 5.3.	Medium	Lower	4/23/2017 (when the Entity failed to revoke access to BCSI)	5/8/2017 (when the Entity corrected the revocation of access issues)	Self-Report	2/15/2018	9/10/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			<p>On █ the Entity submitted a Self-Report stating that, as a █, it was in violation of CIP-004-6 R5, Part 5.3.</p> <p>The Entity did not revoke an individual’s access to the designated storage locations for BES Cyber System Information (BCSI), whether physical or electronic, by the end of the next calendar day following the effective date of the termination action as required by CIP-004-6 R5, Part 5.3.</p> <p>As initially self-reported, the violation started on Sunday, April 23, 2017, which was one calendar day after the individual’s last day of a two-week notice. The violation ended on Monday, April 24, 2017 when the “personnel out” process was completed, two days after termination.</p> <p>During the extent of condition review, an additional four (4) occurrences were discovered dating back to the July 1, 2016, enforcement date of the Standard, with an end date of May 8, 2017. During the period of the violation, 39 terminations were processed and five (5) of these were not completed in accordance with the Standard.</p> <p>The contributing causes for this violation were the failure to follow the Entity process for personnel termination, a lack of internal controls, and insufficient management oversight during the revocation process.</p>						
<b>Risk Assessment</b>			<p>This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The Entity’s failure to revoke terminated employees' physical or electronic access could have led to unauthorized access to BCSI. None of the terminations were for cause, and the duration of each instance was not greater than two (2) days.</p> <p>No harm is known to have occurred.</p>						
<b>Mitigation</b>			<p>To mitigate this violation, the Entity:</p> <ul style="list-style-type: none"><li>1) revoked access for cases where access revocation was not completed in required time;</li><li>2) updated process to include emergency access revocation steps by System Access Administrators;</li><li>3) included access revocation process training for required employees;</li><li>4) modified the access revocation process checklist for confirmation of terminations and retirements, that must be submitted by the user or user's manager prior to last day working;</li><li>5) completed a root cause analysis; and</li><li>6) performed an extent of condition evaluation.</li></ul>						
<b>Other Factors</b>			<p>The Region reviewed the Entity's compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.</p>						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017869	CIP-007-6	R1., 1.1.	Medium	Severe	7/1/2016 (when the Entity failed to properly document ports and services as required by CIP Version 5)	3/30/2018 (when the Entity corrected baselines of all assets identified)	Self-Report	3/30/2018	9/24/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █, the Entity submitted a Self-Report stating that, as a █, it had a violation of CIP-007-6 R1, Part 1.1.  This violation started on July 1, 2016, the effective date of Standard, when the Entity failed to properly determine logical network accessible port ranges or services needed to handle dynamic ports on seven (7) Electronic Access Control or Monitoring (EACM) Cyber Assets.  Specifically, the Entity approved use of █ for █ authentication even though the Entity does not utilize any █ system.  During an extent of condition review, the Entity determined that an additional 61 Cyber Assets had active ports and services that were not documented in the baseline correctly. The entity had a total of 68 Cyber Assets with incorrectly documented ports and services.  The causes for this violation were the incorrect interpretation of the procedure by the Subject Matter Expert (SME), inadequate internal controls, no documented testing requirements and insufficient management oversight during the ports and services authentication process.						
<b>Risk Assessment</b>			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  The Entity’s failure to document the needed logical network accessible ports on BES Cyber Systems and their associated EACMs, PACS, and PCAs could have allowed unauthorized entry into those Cyber Assets, causing an impact to the BPS.  The risk was reduced because █ was not enabled on any of the devices. The Entity does not use █ and instead uses █  Although the ports and services discovered in the extent of condition were all determined to be needed by the Entity, the proper process to document was not completed.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) corrected baselines of all assets identified with incorrect baselines; 2) revised CIP Policy to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations; 3) enhanced controls to ensure that all baselines are reviewed for every entry and justifications are documented during initial commissioning test cycle; 4) updated procedure to ensure that ports are identified based on network accessibility and not port communication state; 5) designed control for periodic review of work products and documented outputs of changes performed by SME; and 6) documented training and acknowledgement from SME for all changes in controls and updates.						
<b>Other Factors</b>			The Region reviewed the Entity's compliance history and determined there were two relevant instances of noncompliance, which were considered to be aggravating: In FRCC201100436, the Entity did not restrict all ports with the exception of only ports required for normal or emergency operations for two devices within the ESP as required by CIP-007-1, R2; and In FRCC2014013357, the Entity discovered it failed to document ports and services required for normal and emergency operations per CIP-007-3a R2; R2.1, R2.2, and R2.3.  The Region determined FRCC2011008528 to not be an aggravating factor as the facts and circumstances are different in that the entity failed to timely submit a Technical Feasibility Exception (TFE). The entity implemented comparable security measures but failed to submit the TFE before the safe harbor date.  The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017375	CIP-007-6	R2., 2.1. 2.2. 2.3.	Medium	Moderate	7/1/2016 (when the Entity failed to implement the patch management processes required by CIP Version 5)	7/13/2018 (when the Entity corrected the patching issues)	Self-Report	7/13/2018	9/27/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			<p>On █, the Entity submitted a Self-Report stating that, as a █, it had an issue of CIP-007-6 R2, Parts 2.1, 2.2 and 2.3.</p> <p>This issue started on July 1, 2016, the effective date of Standard, when:</p> <p>1) the Entity failed to follow its patch management process for tracking cyber security patches for applicable Cyber Assets as required by CIP-007-6 R2, Part 2.1;</p> <p>2) the Entity failed to, at least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 as required by CIP-007-6 R2, Part 2.2; and</p> <p>3) the Entity failed to, within 35 calendar days of the evaluation completion, take one of the following actions: apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan as required by CIP-007-6 R2, Part 2.3.</p> <p>During the extent of condition review, the Entity determined it failed to follow the patch management process on 110 devices (101 High Impact Assets and nine (9) Medium Impact Assets).</p> <p>The causes for this violation were a failure to follow the Entity's process, poorly documented internal controls and lack of internal controls during the verification and periodic review.</p>						
<b>Risk Assessment</b>			<p>This violation posed a serious risk to the reliability of the bulk power system (BPS).</p> <p>The Entity’s failure to execute its patch management process could have prolonged the presence of software vulnerabilities, which, if exploited, could grant access to unauthorized personnel or misuse of the Cyber Assets, impacting the reliability of the BPS.</p>						
<b>Mitigation</b>			<p>To mitigate this violation, the Entity:</p> <p>1) completed patch review for all devices to include all patches released until date for all devices determined as non-compliant for this Self-Report;</p> <p>2) implemented patches that are assessed as applicable in step 1 or created Mitigation Plans;</p> <p>3) updated the procedure to include controls for the following:</p> <p>    a. 31-day patch review/assessment for applicability from the date of last patch assessment for all patch releases since last patch assessment</p> <p>    b. 31-day implementation or mitigation starting from the date of completion of patch assessment</p> <p>    c. Application inventory tracking to ensure that all applications are being tracked for patches and updates;</p> <p>4) documented and implemented controls to ensure that all supporting evidence is stored and reviewed for accuracy periodically by SME peers or managers and verified by compliance;</p> <p>5) trained employees on new process, tools, and internal controls;</p> <p>6) completed root cause analysis to identify root cause of noncompliance;</p> <p>7) completed activities necessary to correct the noncompliance; and</p> <p>8) performed an extent of condition evaluation.</p>						
<b>Other Factors</b>			<p>The Region reviewed the Entity's compliance history and determined there were two (2) relevant instances of noncompliance, which were considered to be aggravating:</p> <p>In FRCC2014013414, the Entity discovered that a technology services analyst failed to complete the documentation of the assessment of the patches for the applicability to the Cyber Asset environment. Multiple security patches were released but the analyst documentation was not sufficient to demonstrate the compliance with the requirement; and</p> <p>In FRCC2011007523, the Entity failed to establish, document and implement a security patch management program for tracking, evaluating, testing, and installing of several third-party applications installed on many of the Cyber Assets within the Electronic Security Perimeter(s).</p> <p>The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations. In Addition, Self-Reporting credit was awarded for violations that were self-reported prior to the entity receiving the audit notification letter.</p>						



NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017833	CIP-007-6	R4., 4.1.	Medium	Severe	7/1/2016 (when the Entity failed to log required events)	4/18/2018 (when the Entity corrected the logging configurations)	Self-Report	4/18/2018	9/13/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █, the Entity submitted a Self-Report stating that, as a █, it was in violation of CIP-007-6 R4, Part 4.1.  This violation started on July 1, 2016, the effective date of Standard, when the Entity failed to log the minimum required events at the BES Cyber System or the Cyber Asset level capability. Specifically, the Entity failed to log events related to successful login attempts, detected failed access attempts and failed login attempts on 17 BES Cyber Asset (BCA) workstations and five (5) Physical Access Control Systems (PACS).  The extent of condition review determined there was a total of 46 assets where the Entity failed to log for events.  The causes for this violation were the failure to follow the process by the Subject Matter Expert (SME), inadequate internal controls, no testing requirement, no periodic review, and insufficient management oversight.						
<b>Risk Assessment</b>			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  Specifically, the Entity’s failure to ensure that logs of system events related to cyber security for those Cyber Assets were in place, exposed the Cyber Assets to a loss of visibility for possible unauthorized access attempts, as well as a loss of the ability to monitor or review successful logins.  The risk was reduced because all the affected Cyber Assets were located within an identified Electronic Security Perimeter where access is restricted to authorized individuals.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) corrected logging configurations and verified for compliance for all requirements of CIP-007, R4; 2) documented controls for review process for all new assets to ensure that evidence meets required minimum deliverables, such as completed checklist, manager sign-offs; 3) documented and implemented controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing by SME peers or managers and verified by compliance; 4) trained applicable employees on new process, tools, and internal controls; 5) completed root cause analysis; and 6) performed an extent of condition evaluation.						
<b>Other Factors</b>			The Region reviewed the Entity's compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017857	CIP-007-6	R5., 5.7.	Medium	Severe	7/1/2016 (when the Entity failed to limit unsuccessful authentication attempts)	1/15/2018 (when the Entity documented controls for review process)	Self-Report	2/15/2018	9/13/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █, the Entity submitted a Self-Report stating that, as a █, it was in violation of CIP-007-6 R5, Part 5.7.  This violation started on July 1, 2016, effective date of Standard, when the Entity failed to limit unsuccessful authentication attempts, alert for unsuccessful authentication attempts, or file a Technical Feasibility Exception. Specifically, the Entity failed to implement controls to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts on the seven (7) Electronic Access Control or Monitoring (EACM) devices as required by CIP-007-6 R5, Part 5.7.  The extent of condition review determined there were an additional two (2) instances of noncompliance for a total of nine (9) High Impact BES Cyber Assets and their associated EACMS and PACS.  The causes for this violation were due to the incorrect interpretation of the procedure by the Subject Matter Expert (SME), lack of internal controls, no documentation of testing requirements, and insufficient management oversight during the access controls process.						
<b>Risk Assessment</b>			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  Specifically, the Entity’s failure to limit unsuccessful authentication attempts or alerting after a certain number of failed authentication attempts, which serves to prevent unauthorized access through an online guessing or brute force attack, could have caused reliability concerns for the Entity and the Region.  The risk was increased due to long-term (594 days) failure to limit unsuccessful authentication attempts on the nine (9) EACM devices.  The risk was reduced as the issue was restricted to only local accounts on the devices.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) corrected the misconfiguration for subject devices to lock the account after five (5) consecutive failed attempts and alert for response; 2) documented controls for review process for all new assets to ensure that evidence meets required minimum deliverables (completed new asset checklist, testing results output, completed and approved baseline, manager sign-offs); 3) updated the procedure to enable requirement that all security devices, where technically and operationally feasible, must be configured to their highest ability; 4) trained applicable employees on new process, tools, and internal controls; 5) completed root cause analysis; and 6) performed an extent of condition evaluation.						
<b>Other Factors</b>			The Region reviewed the Entity's compliance history and determined the previous instances of noncompliance related to CIP-007 R5 were not relevant and not considered to be aggravating. This includes FRCC2011007519, FRCC2011008529 and FRCC2014013358. CIP-007-6 R5.7 is a new addition to CIP-007-6 R5 with the new version. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						



NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017376	CIP-010-2	R1., 1.1.	Medium	High	7/1/2016 (when the Entity failed to develop proper baselines)	11/15/2017 (when the Entity corrected the baseline configuration issues)	Self-Report	2/15/2018	9/11/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			<p>On █ the Entity submitted a Self-Report stating that, as a █, it was in violation of CIP-010-2 Requirement 1, Part 1.1 and Part 1.2</p> <p>This violation started on July 1, 2016, effective date of the Standard, when the Entity failed to develop baseline configurations for five (5) Intrusion Protection System (IPS) Cyber Assets and failed to document changes from the existing baselines on seven (7) Security Information and Event Management devices (SIEMs).</p> <p>Specifically, for Part 1.1, the five (5) IPS Cyber Assets were modules contained within the same firewall chassis, which the Entity incorrectly considered as one (1) Cyber Asset. Therefore, the Entity did not create the appropriate baselines for the five (5) separate IPS Cyber Assets as required by CIP-010-2 R1, Part 1.1.</p> <p>For Part 1.2, for seven (7) SIEM devices, the Entity failed to authorize changes that deviated from the existing baseline configuration as required by CIP-010-2 R1, Part 1.2.</p> <p>During the extent of condition review, it was determined that the Entity did not authorize changes to the baseline configurations for 61 additional Cyber Assets resulting in a total of 68 Cyber Assets in this violation.</p> <p>The causes for this issue were an incomplete process (1.1) and a lack of internal controls to ensure authorization of changes and updates to baselines occurred (1.2).</p>						
<b>Risk Assessment</b>			<p>This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).</p> <p>The Entity’s failure to develop baselines for the identified Cyber Assets or authorize changes to baseline configurations could have introduced unknown security vulnerabilities within the Cyber Assets and allowed for potential misuse or unavailability of Cyber Assets to occur impacting the reliability of the BPS.</p>						
<b>Mitigation</b>			<p>To mitigate this violation, the Entity:</p> <ul style="list-style-type: none"><li>1) corrected and approved baselines;</li><li>2) completed verification by compliance department;</li><li>3) documented controls for review process for all assets to ensure that evidence meets required minimum deliverables (completed new asset checklist, testing results output, completed and approved baseline, manager sign-offs);</li><li>4) documented and implemented controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance;</li><li>5) trained employees on new process, tools, and internal controls;</li><li>6) completed a root cause analysis; and</li><li>7) performed an extent of condition evaluation.</li></ul>						
<b>Other Factors</b>			<p>The Region reviewed the Entity's compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations. In Addition, Self-Reporting credit was awarded for violations that were self-reported prior to the entity receiving the audit notification letter.</p>						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017835	CIP-010-2	R3., 3.3.	Medium	Severe	12/1/2016 (when the Entity failed to perform an active vulnerability assessment as required following the addition of two switches)	6/27/2017 (when the vulnerability assessment was performed)	Self-Report	1/15/2018	9/24/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █, the Entity submitted a Self-Report stating that, as a █, it was in violation of CIP-010-2 R3, Part 3.3.  This violation started on December 1, 2016, when the Entity added two (2) switches, to manage network isolation of the production environment, as Protected Cyber Assets (PCAs) without performing a vulnerability assessment as required by CIP-010-2 R3 Part 3.3.  During an extent of condition review, the Entity discovered no additional occurrences dating back to the July 1, 2016 enforcement date.  The causes for this violation were an incomplete documented procedure, lack of internal controls and insufficient management oversight during the configuration change management process.						
<b>Risk Assessment</b>			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  Specifically, the Entity’s failure to perform a vulnerability assessment on all Cyber Assets prior to placing them into a production environment could have allowed for malicious code or virus intrusion via malware on the Entity’s network(s). This could have caused an impact to the BPS.  The risk was reduced as the device at issue provided increased threat response capability to isolate the network if necessary. In addition, a subsequent vulnerability assessment was performed and revealed no vulnerabilities.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) performed required vulnerability assessment and review by the Entity compliance; 2) documented controls for review process for all new assets to ensure that evidence meets required minimum deliverables (completed new asset checklist, testing results output, completed and approved baseline, manager sign-offs); 3) updated procedure and controls to ensure all new asset implementation includes Security Assessment Scan and documentation of results, which are stored for the Entity compliance verification; 4) documented and implemented controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by peer or manager and verified by the Entity compliance; 5) trained employees on new process, tools, and internal controls; 6) performed a root cause analysis; and 7) performed an extent of condition evaluation.						
<b>Other Factors</b>			The Region reviewed the Entity’s compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
FRCC2017017696	CIP-011-2	R1., 1.1.	Medium	Severe	7/1/2016 (when the Entity failed to implement a program for BCSI)	1/10/2018 (when the Entity created and implemented the process and properly identified all BCSI storage locations)	Self-Report	2/15/2018	9/11/2018
<b>Description of the Violation (For purposes of this document, each violation at issue is described as a “violation,” regardless of its procedural posture and whether it was a possible, or confirmed violation.)</b>			On █, the Entity submitted a Self-Report stating that, as a █ it was in violation of CIP-011-2 R1.  This violation started on July 1, 2016, when the Entity failed to implement one or more documented information protection program(s) that would identify all storage locations that included BES Cyber System Information (BCSI) as required by CIP-011-2 R1.1.  The Entity’s extent of condition review determined that it did not identify five (5) servers as storage locations of BCSI.  The causes for this violation were due to the incorrect interpretation of the Standard by the Subject Matter Expert (SME), no documented procedure, lack of internal controls, and insufficient management oversight during the BCSI identification process.						
<b>Risk Assessment</b>			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).  The Entity’s failure to identify 71% of the storage locations that included BCSI could have allowed unauthorized access or misuse of BCSI, which could lead to exploitation of Cyber Assets and intrusion of the Entity’s secure network, potentially impacting the reliability of the BPS.  The risk was reduced as the five (5) servers did not contain any BCA operating or functional images, nor BCA credentials or hashes. Additionally, all users of the systems have CIP certifications, training, and Personnel Risk Assessments.						
<b>Mitigation</b>			To mitigate this violation, the Entity: 1) updated the list of all Cyber Assets that contain BCSI; 2) performed compliance review and implemented required security controls; 3) revised CIP Policy to add requirements for SME Compliance Responsibilities and specified process and ownership for resolution of Compliance Interpretations; 4) created and implemented formal BCSI asset identification process, including deliverables such as survey submitted to all SME department heads annually; 5) created and implemented controls for annual review and independent review by compliance department; 6) created controls and implemented an Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied; 7) trained employees on new processes, tools, and internal controls; 8) performed a root cause analysis; and 9) performed an extent of condition evaluation.						
<b>Other Factors</b>			The Region reviewed the Entity's compliance history and determined there are no previous instances of noncompliance. The Region reviewed the Entity’s Internal Compliance Program (ICP) and awarded minimal credit for the ICP. While the ICP allowed the issues to occur, it also allowed the entity to operate reliably during the pendency of the violations.						

## Attachment 3

- 3a. The Entity's Mitigation Plan designated as FRCCMIT013372 for CIP-004-6 R4 submitted November 9, 2017;
- 3b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted June 12, 2018;
- 3c. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated September 10, 2018;

 A [previous version](#) of this Mitigation Plan exists

 This item was signed by [REDACTED] on 11/9/2017

 This item was marked ready for signature by [REDACTED] on 10/30/2017

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

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

Name:

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

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

Standard: CIP-004-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R4.	FRCC2017-100936	FRCC2017017834	[REDACTED]

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

[REDACTED] is self-reporting a violation of CIP-004 R4.1 as it failed to authorize the electronic access for the following two instances:

- One network admin gained access to [REDACTED] High Impact CIP EACM without first receiving proper authorization.
- For two individuals, normal and admin user accounts were added to a [REDACTED] High Impact CIP Cyber Asset. However, authorization was only received for the admin account not the user's personal account.

[REDACTED] also considers that attestation process that has appended prior to compliance period is sufficient for authorization and such cases are not violation of CIP-004, R4.1 and are not included in any report.

Further [REDACTED] self reported R4.2 after it conducted a compliance review and determined that the process implemented to comply with CIP-004, R4.2 was incorrectly implemented and legacy CIP Version 3 process was continued. Due to subtle change in standard and requirement, and SME oversight, [REDACTED] failed to verify for three calendar quarters that individuals with active electronic access or unescorted physical access have authorization records. Instead [REDACTED] continued the practice of System Owner Attestation to verify the continued need for Access Authorization.

[Attachments \(\)](#)

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

all users had proper CIP PRA and Training and violation occurred due to insufficient controls.

[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, or correct the Alleged or Confirmed violations identified above in Part C.1 of this form:

1. Complete quarterly review (11/15/2017)
2. Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS) and revoke access for users who do not require access or can't be authorized in a timely manner (Complete - 11/15/2017).
3. Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account and document quarterly review for authorization process. (11/15/2017 - IS)
4. Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege. (11/15/2017 - IS)
5. Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS)
6. Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)
7. Complete Extent of condition review (12/15/2017)
8. Identify Root Cause for Violation (11/30/2017)
9. Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

#### 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:

1/31/2018

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

Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS)

Milestone Pending (Due: 11/15/2017)

1. Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS), and revoke access for users who do not require access or can't be authorized in a timely manner (Complete - 08-2017).

Complete quarterly review (11/15/2017)

Milestone Pending (Due: 11/15/2017)

Complete quarterly review for authorization for all active users CIP-004, R4.2 (11/15/2017)

Update Procedure for explicit guidance and include control for CIP group selections

Milestone Pending (Due: 11/15/2017)

Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account and document quarterly review for authorization process. (11/15/2017 - IS)

Complete Extent of condition review (12/15/2017)

Milestone Pending (Due: 11/15/2017)

Complete Extent of condition review (12/15/2017)

Complete Root Cause Analysis

Milestone Pending (Due: 11/15/2017)

Complete Root Cause Analysis (11/15/2017)

Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege.

Milestone Pending (Due: 12/15/2017)

Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege. (11/15/2017 - IS)

Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS)

Milestone Pending (Due: 12/15/2017)

Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS)

Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)

Milestone Pending (Due: 12/15/2017)

Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

Milestone Pending (Due: 1/30/2018)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

#### 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):

conducted the review and assessed minimal risk as all users were already approved under other previous requests. This issue was merely a documentation issue.

[Attachments \( \)](#)

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

Additional controls are being designed to limit future risk of violations.

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

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/12/2018

This item was marked ready for signature by [REDACTED] on 6/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-004-6

Requirement	Tracking Number	NERC Violation ID
R4.	FRCC2017-100936	FRCC2017017834

Date of completion of the Mitigation Plan:

1/30/2018

[Correct the current access group to only include authorized users only and obtain authorization for required members \(10/27/17 - IS\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 7/31/2017)

[Attachments \(0\)](#)

1. Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS), and revoke access for users who do not require access or can't be authorized in a timely manner (Complete - 08-2017).

[Complete quarterly review \(11/15/2017\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 10/31/2017)

[Attachments \(0\)](#)

Complete quarterly review for authorization for all active users CIP-004, R4.2 (11/15/2017)

[Update Procedure for explicit guidance and include control for CIP group selections](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account and document quarterly review for authorization process. (11/15/2017 - IS)

[Complete Extent of condition review \(12/15/2017\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Complete Extent of condition review (12/15/2017)

[Complete Root Cause Analysis](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Complete Root Cause Analysis (11/15/2017)

[Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege.](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege. (11/15/2017 - IS)

[Update procedure to document alternate means of authorization approval such as Multiple user \(grouped by project\), using change ticket, etc. \(12/15/2017 - IS\)](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS)



[Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. \(12/15/2017 - IS\)](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)  
[Attachments \(0\)](#)

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

Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)

[Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls \(1/30/2018\)](#)

Milestone Completed (Due: 1/30/2018 and Completed 1/30/2018)  
[Attachments \(0\)](#)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

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

████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

**Description of the information provided to FRCC for their evaluation \***

████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

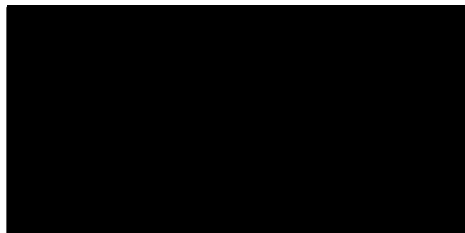


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 10, 2018



Re: [REDACTED] ( [REDACTED] )  
**Mitigation Plan Verification of Completion  
FRCC2017017834 (CIP-004-6 R4)**

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED] ( [REDACTED] ) for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017834	CIP-004-6 R4	June 12, 2018

After review for completion on **September 7, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 4

- 4a. The Entity's Mitigation Plan designated as FRCCMIT013384 for CIP-004-6 R4 submitted November 16, 2017;
- 4b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R4 submitted June 12, 2018;
- 4c. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R4 dated September 10, 2018;

 A [previous version](#) of this Mitigation Plan exists

 This item was signed by [REDACTED] on 11/16/2017

 This item was marked ready for signature by [REDACTED] on 11/13/2017

SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

SECTION B: REGISTERED ENTITY INFORMATION

B.1 Identify your organization

Company Name:

Company Address:

Compliance Registry ID:

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

Name:

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

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

Standard:

CIP-004-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R4.	FRCC2017-100921	FRCC2017017370	[REDACTED]

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

following a compliance review it was determined that the process implemented to comply with CIP-004, R4.2 was incorrectly implemented and legacy CIP Version 3 process was continued. Due to subtle change in standard and requirement, and SME oversight, [REDACTED] failed to verify for three calendar quarters that individuals with active electronic access or unescorted physical access have authorization records. Instead [REDACTED] continued the practice of System Owner Attestation to verify the continued need for Access Authorization.

[Attachments \(\)](#)

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

This violation has been corrected. This mitigation plan milestones and activities are combined with CIP-004 R4.1 activities as they are interlinked.

[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:

1. Correct access issues after completion of quarterly authorization (11/30/2017).
2. Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account. (11/15/2017 - IS)
4. Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege. (11/15/2017 - IS)



5. Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS)
6. Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)
7. Complete Extent of condition review (12/15/2017)
8. Identify Root Cause for Violation (11/30/2017)
9. Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

NON-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:

1/30/2018

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

Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account. (11/15/2017 - IS)

Milestone Pending (Due: 11/15/2017)

Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account. (11/15/2017 - IS)

Complete Extent of condition review (11/15/2017)

Milestone Pending (Due: 11/15/2017)

Complete Extent of condition review (11/15/2017)

Report any additional deficiencies to FRCC

Milestone Pending (Due: 11/30/2017)

Correct and Report any additional deficiencies to FRCC. (July 31, 2017)

Correct the current access issues identified during audit or after completion of quarterly review for authorizations (Complete - 11/30/2017).

Milestone Pending (Due: 11/30/2017)

After the quarterly review is complete, correct access issues for which no record exists. Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS), and revoke access for users who do not require access or can't be authorized in a timely manner (Complete - 11/30/2017).

Identify Root Cause for Violation (11/30/2017)

Milestone Pending (Due: 11/30/2017)

Identify Root Cause for Violation (11/30/2017)

Update procedure controls for administrative accounts and alternate means of authorizations (multi-User)

Milestone Pending (Due: 12/15/2017)

Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege and Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS).

Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)

Milestone Pending (Due: 12/15/2017)

Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. (12/15/2017 - IS)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

Milestone Pending (Due: 1/30/2018)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

#### 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):

█ has completed the review and determined that no unauthorized access was allowed. Only authorization records were missing and that issue is being corrected.

#### Attachments ()

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

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

#### SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/12/2018

This item was marked ready for signature by [REDACTED] on 6/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-004-6

Requirement	Tracking Number	NERC Violation ID
R4.	FRCC2017-100921	FRCC2017017370

Date of completion of the Mitigation Plan:

1/30/2018

[Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account. \(11/15/2017 - IS\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Update procedure to state that all accounts access must be requested and approved, even if the account that belongs to user already approved under separate account. (11/15/2017 - IS)

[Complete Extent of condition review \(11/15/2017\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Complete Extent of condition review (11/15/2017)

[Report any additional deficiencies to FRCC](#)

Milestone Completed (Due: 11/30/2017 and Completed 7/31/2017)

[Attachments \(0\)](#)

Correct and Report any additional deficiencies to FRCC. (July 31, 2017)

[Correct the current access issues identified during audit or after completion of quarterly review for authorizations \(Complete - 11/30/2017\).](#)

Milestone Completed (Due: 11/30/2017 and Completed 11/30/2017)

[Attachments \(0\)](#)

After the quarterly review is complete, correct access issues for which no record exists. Correct the current access group to only include authorized users only and obtain authorization for required members (10/27/17 - IS), and revoke access for users who do not require access or can't be authorized in a timely manner (Complete - 11/30/2017).

[Identify Root Cause for Violation \(11/30/2017\)](#)

Milestone Completed (Due: 11/30/2017 and Completed 12/27/2017)

[Attachments \(0\)](#)

Identify Root Cause for Violation (11/30/2017)

[Update procedure controls for administrative accounts and alternate means of authorizations \(multi-User\)](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

Update controls to ensure that administrative accounts are limited for administration only and user only accounts are not allowed administrative privilege and Update procedure to document alternate means of authorization approval such as Multiple user (grouped by project), using change ticket, etc. (12/15/2017 - IS).

[Document single verifiable reference sources used for authorization approval and ensure that they are maintained and up to date, e.g. Shared Accounts listing, EMS to corporate authorized group translation document etc. \(12/15/2017 - IS\)](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

[Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls \(1/30/2018\)](#)

Milestone Completed (Due: 1/30/2018 and Completed 1/30/2018)

[Attachments \(0\)](#)

Complete training or certification of acknowledgement for subject SME for understanding of newly designed controls (1/30/2018)

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

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.



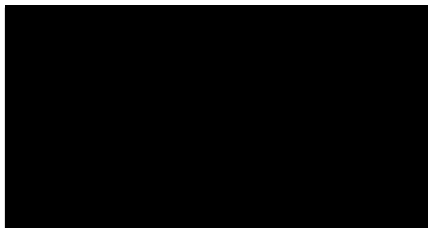


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 10, 2018



Re: [REDACTED] ( [REDACTED] )  
**Mitigation Plan Verification of Completion  
FRCC2017017370 (CIP-004-6 R4)**

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED] ( [REDACTED] ) for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017370	CIP-004-6 R4	June 12, 2018

After review for completion on **September 7, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.


Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 5


- 5a. The Entity's Mitigation Plan designated as FRCCMIT013371 for CIP-004-6 R5 submitted November 9, 2017;
- 5b. The Entity's Certification of Mitigation Plan Completion for CIP-004-6 R5 submitted June 12, 2018;
- 5c. FRCC's Verification of Mitigation Plan Completion for CIP-004-6 R5 dated September 10, 2018;

 A [previous version](#) of this Mitigation Plan exists



 This item was signed by [REDACTED] on 11/9/2017



 This item was marked ready for signature by [REDACTED] on 10/25/2017



## SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

### B.1 Identify your organization

Company Name:

[REDACTED]

Company Address:

[REDACTED]

[REDACTED]

Compliance Registry ID:

[REDACTED]

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

Name:

[REDACTED]

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

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

Standard:

CIP-004-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	FRCC2017-100924	FRCC2017017454	[REDACTED]

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

[REDACTED] is self-reported this violation as one of the [REDACTED] personnel (IT Projects) who had access to [REDACTED] BCSI information submitted her resignation on April 10, 2017 with two week notice. This person's last day at work was on Friday, April 21, 2017, however [REDACTED] failed to revoke her access by next calendar day. This violation resulted from human error as Reporting Manager did not initiate the [REDACTED] Personnel Out Process (POP) and only initiated the POP on April 24, 2017. Individual's access was revoked on April 24, 2017.

The subject individual was employed with [REDACTED] for a long career and is being rehired as contractor with expected start date of April 25, 2017.

[Attachments \(\)](#)

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

The violation happened because of Oversight of the Reporting Manager. Reporting Manager failed to initiate the Access Termination Request and as a result, a two day violation happened.

[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: Access has been revoked on April 24, 2017.

Details to Prevent Recurrence: Meeting is scheduled with the Director Projects to discuss prevention of reoccurrence.

Following the meeting, the Reporting Manager stated that they understand the issue and best efforts will be made to limit risk of any such violation in the future.



#### 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:

2/15/2018

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

#### Complete a Root Cause Analysis (4/30/2017)

Milestone Pending (Due: 4/30/2017)

RCA was completed and determined that SMA Manager's oversight (Human Error) was the root cause of the violation.

#### 1. Revoke access for cases where access revocation was not completed in required time (Complete).

Milestone Completed (Due: 5/9/2017 and Completed 5/9/2017)

Access was revoked for the cases.

FRCC2017017454 212 [REDACTED] - 7/2/2016 (required by 7/1/2016)  
FRCC2017017454 101842 [REDACTED] - 5/9/2017 (Required by 5/8/2017)  
FRCC2017017454 131 [REDACTED] - 4/27/2017 (Required by 4/25/2017)

#### Perform an extent of condition evaluation

Milestone Completed (Due: 5/31/2017 and Completed 5/31/2017)

Extent of condition - Analysis was completed and additional two issues were identified and corrected. All issues resulted from human error/oversight.

#### 3. Include POP process training for all employees. (12/30/2017)

Milestone Pending (Due: 12/31/2017)

Every year CIP training is refreshed. Details of POP (Personnel Out Process) will be included in the annual training for 2018, which is completed by January-February of 2018.

#### 2. Update process and provision emergency access revocation steps that can revoke CIP access on demand by System Access Administrators. (1/15/2018 - IS)

Milestone Pending (Due: 1/15/2018)

Update the procedure, that if proper approval is available, Information Access Control group can terminate all CIP access, using emergency action. This will require program change to the [REDACTED] provisioning system.

#### 4. Work with HR for POP process checklist for confirmation for all terminations and retirements, that must be submitted by the user or User Manager prior to last day working (Badges, Confidential Info, Two Factor Fob etc.). (2/15/2018 - IS & TI)

Milestone Pending (Due: 2/15/2018)

4. Work with HR for POP process checklist for confirmation for all terminations and retirements, that must be submitted by the user or User Manager prior to last day working (Badges, Confidential Info, Two Factor Fob etc.). (2/15/2018 - IS & TI)

### 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):

There was minimal risk. Violations were just a day or two. All violations have been corrected.

#### Attachments ()

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

[REDACTED] is updating procedures to limit impact of human errors or limit risk of oversight.

#### 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 FRCC 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]
  - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
  - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
  - I have read and am familiar with the contents of this Mitigation Plan
  - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

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

#### SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/12/2018

This item was marked ready for signature by [REDACTED] on 6/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-004-6

Requirement	Tracking Number	NERC Violation ID
R5.	FRCC2017-100924	FRCC2017017454

Date of completion of the Mitigation Plan:

2/15/2018

Complete a Root Cause Analysis (4/30/2017)

Milestone Completed (Due: 4/30/2017 and Completed 4/30/2017)

[Attachments \(0\)](#)

RCA was completed and determined that SMA Manager's oversight (Human Error) was the root cause of the violation.

1. Revoke access for cases where access revocation was not completed in required time (Complete).

Milestone Completed (Due: 5/9/2017 and Completed 4/24/2017)

[Attachments \(0\)](#)

Access was revoked for the cases.

FRCC2017017454 212 [REDACTED] - 7/2/2016 (required by 7/1/2016)  
FRCC2017017454 101842 [REDACTED] - 5/9/2017 (Required by 5/8/2017)  
FRCC2017017454 1311 [REDACTED] - 4/27/2017 (Required by 4/25/2017)

Perform an extent of condition evaluation

Milestone Completed (Due: 5/31/2017 and Completed 5/31/2017)

[Attachments \(0\)](#)

Extent of condition - Analysis was completed and additional two issues were identified and corrected. All issues resulted from human error/oversight.

3. Include POP process training for all employees. (12/30/2017)

Milestone Completed (Due: 12/31/2017 and Completed 12/31/2017)

[Attachments \(0\)](#)

Every year CIP training is refreshed. Details of POP (Personnel Out Process) will be included in the annual training for 2018, which is completed by January-February of 2018.

2. Update process and provision emergency access revocation steps that can revoke CIP access on demand by System Access Administrators. (1/15/2018 - IS)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

Update the procedure, that if proper approval is available, Information Access Control group can terminate all CIP access, using emergency action. This will require program change to the [REDACTED] provisioning system.

4. Work with HR for POP process checklist for confirmation for all terminations and retirements, that must be submitted by the user or User Manager prior to last day working (Badges, Confidential Info, Two Factor Fob etc.). (2/15/2018 - IS & TI)

Milestone Completed (Due: 2/15/2018 and Completed 2/6/2018)

[Attachments \(0\)](#)

4. Work with HR for POP process checklist for confirmation for all terminations and retirements, that must be submitted by the user or User Manager prior to last day working (Badges, Confidential Info, Two Factor Fob etc.). (2/15/2018 - IS &amp; TI)

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

████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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

Description of the information provided to FRCC for their evaluation \*

████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.



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

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 10, 2018

Re: [REDACTED] ( [REDACTED] )  
**Mitigation Plan Verification of Completion  
FRCC2017017454 (CIP-004-6 R5)**

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED] ( [REDACTED] ) for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017454	CIP-004-6 R5	June 12, 2018

After review for completion on **September 7, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma



## Attachment 6

- 6a. The Entity's Mitigation Plan designated as FRCCMIT013376 for CIP-007-6 R1 submitted November 9, 2017;
- 6b. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R1 submitted July 18, 2018;
- 6c. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R1 dated September 24, 2018;

This item was signed by [REDACTED] on 11/9/2017

This item was marked ready for signature by [REDACTED] on 10/22/2017

## SECTION A: COMPLIANCE NOTICES &amp; MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

## B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]  
[REDACTED]

Compliance Registry ID: [REDACTED]

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

Name: [REDACTED]

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

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

Standard:

CIP-007-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	FRCC2017-100939	FRCC2017017869	[REDACTED]

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

[REDACTED] is self reporting CIP-007, R1 as it failed to 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. [REDACTED] approved use of [REDACTED] used for [REDACTED] authentication when [REDACTED] does not utilize any [REDACTED] system. [REDACTED] also failed to identify outbound ports and dynamic ports on the required ports listing due to SME misinterpretation of standards.

[Attachments \(\)](#)

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

[REDACTED] conducted assessment of multiple assets and identified that 26 assets were not in compliance, including HMI workstations, EMS Servers, AD servers, SIEM, EACMs, and PACS.

[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:

1. Correct baselines of all assets identified with incorrect baselines (12/15/2017 - IS & TI).
2. Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp)
3. Enhance controls to ensure that all baselines are reviewed for every entry and justifications are documented during initial commissioning test cycle (12/15/2017 - IS & TI).
4. Update procedure to ensure that ports are identified based on network accessibility and not port communication state (1/15/2018 - IS & TI).
5. Design control for periodic review of work products and documented outputs of changes performed by SME (NLT Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually) (3/15/2018 - TI).

[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:

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

3/30/2018

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

Extent of condition review for the balance of assets where the violation may exist.

Milestone Pending (Due: 11/10/2017)

Extent of condition review for the balance of assets where the violation may exist.

1. Correct baselines of all assets identified with incorrect baselines (11/15/2017 - IS & TI).

Milestone Pending (Due: 11/15/2017)

Due to incorrect Ports information, many baselines are incorrect. [REDACTED] will correct the ports information for the baselines.

2. Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp)

Milestone Pending (Due: 11/15/2017)

MD 202 is core governance policy and its important to update the policy to specify organizational ownership and responsibility, which will help us build the accountability.

RCA for identified Issues

Milestone Pending (Due: 11/15/2017)

Root cause analysis for issues identified for SR and Extent of condition review

3. Enhance controls to ensure that all baselines are reviewed for every entry and justifications are documented during initial commissioning test cycle (12/15/2017 - IS & TI).

Milestone Pending (Due: 12/15/2017)

Correct the procedure that will help [REDACTED] limit future issues.

4. Update procedure to ensure that ports are identified based on network accessibility and not port communication state (1/15/2018 - IS & TI).

Milestone Pending (Due: 1/15/2018)

Update procedure to ensure that ports are identified based on network accessibility and not port communication state and this will ensure that outbound ports.

5. Design control for periodic review of work products and documented outputs of changes performed by SME (NLT Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually) (3/15/2018 - TI).

Milestone Pending (Due: 3/15/2018)

5. Design control for periodic review of work products and documented outputs of changes performed by SME, requiring reviews no later than (NLT) Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually)

Training or Acknowledgement from SME for all changes in controls and updates for limiting the risk of future violations.

Milestone Pending (Due: 3/30/2018)

Training or Acknowledgement from SME for all changes in controls and updates for limiting the risk of future violations.

## 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):

we have reviewed our firewall configs to limit any impact. Many issues were documentations only and for the rest issues are being reviewed in logs.

[Attachments \(\)](#)

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

3. Enhance controls to ensure that all baselines are reviewed for every entry and justifications are documented during initial commissioning test cycle (12/15/2017 - IS & TI).

4. Update procedure to ensure that ports are identified based on network accessibility and not port communication state (1/15/2018 - IS & TI).

5. Design control for periodic review of work products and documented outputs of changes performed by SME (NLT Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually) (3/15/2018 - TI).

These milestones are designed to limit future risk of violations.

[Attachments \(\)](#)



## SECTION F: AUTHORIZATION

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

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

## SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com

This item was signed by [REDACTED] on 7/18/2018

This item was marked ready for signature by [REDACTED] on 7/17/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-007-6

Requirement	Tracking Number	NERC Violation ID
R1.	FRCC2017-100939	FRCC2017017869

Date of completion of the Mitigation Plan:

3/30/2018

[Extent of condition review for the balance of assets where the violation may exist.](#)

Milestone Completed (Due: 11/10/2017 and Completed 9/28/2017)

[Attachments \(0\)](#)

Extent of condition review for the balance of assets where the violation may exist.

[1. Correct baselines of all assets identified with incorrect baselines \(11/15/2017 - IS & TI\).](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Due to incorrect Ports information, many baselines are incorrect. [REDACTED] will correct the ports information for the baselines.

[2. Revise CIP Policy \(MD-202\) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. \(11/15/2017 - Comp\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

MD 202 is core governance policy and its important to update the policy to specify organizational ownership and responsibility, which will help us build the accountability.

[RCA for identified Issues](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Root cause analysis for issues identified for SR and Extent of condition review

[3. Enhance controls to ensure that all baselines are reviewed for every entry and justifications are documented during initial commissioning test cycle \(12/15/2017 - IS & TI\).](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

Correct the procedure that will help [REDACTED] limit future issues.

[4. Update procedure to ensure that ports are identified based on network accessibility and not port communication state \(1/15/2018 - IS & TI\).](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

Update procedure to ensure that ports are identified based on network accessibility and not port communication state and this will ensure that outbound ports.

[5. Design control for periodic review of work products and documented outputs of changes performed by SME \(NLT Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually\) \(3/15/2018 - TI\).](#)

Milestone Completed (Due: 3/15/2018 and Completed 1/22/2018)

[Attachments \(0\)](#)

5. Design control for periodic review of work products and documented outputs of changes performed by SME, requiring reviews no later than (NLT) Manager Lvl - 3 Months, Director Lvl - 6 Months, Compliance - Annually)

[Training or Acknowledgement from SME for all changes in controls and updates for limiting the risk of future violations.](#)

Milestone Completed (Due: 3/30/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

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

Training or Acknowledgement from SME for all changes in controls and updates for limiting the risk of future violations.

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

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.





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

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 24, 2018

Re: [REDACTED] ( [REDACTED] )  
**Mitigation Plan Verification of Completion  
FRCC2017017869 (CIP-007-6 R1)**

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED] ( [REDACTED] ) for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017869	CIP-007-6 R1	July 18, 2018

After review for completion on **September 21, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.


Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 7

- 7a. The Entity's Mitigation Plan designated as FRCCMIT013383 for CIP-007-6 R2 submitted November 16, 2017;
- 7b. The Entity's Request for Mitigation Plan Extension for CIP-007-6 R2 submitted June 18, 2018;
- 7c. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R2 submitted July 19, 2018;
- 7d. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R2 dated September 27, 2018;

 A [previous version](#) of this Mitigation Plan exists  This item was signed by [REDACTED] on 11/16/2017  This item was marked ready for signature by [REDACTED] on 11/15/2017 **SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS**

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

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

**SECTION B: REGISTERED ENTITY INFORMATION****B.1 Identify your organization**

Company Name: [REDACTED]

Company Address: [REDACTED]  
[REDACTED]

Compliance Registry ID: [REDACTED]

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

Name: [REDACTED]

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

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

Standard:	CIP-007-6		
Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R2.	FRCC2017-100923	FRCC2017017375	[REDACTED]

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

[REDACTED] is self reporting that it failed to comply with CIP-007, R2 for the following issues -

- 2.1. SMEs failed to track two applications for patching.
- 2.2. For five application either the patch review not conducted within the 35 days as required by CIP-007, R2.2 or failed to correctly assess a security patch/update.
- 2.3. For three instances [REDACTED] SME failed to complete the installation within 35 days as required by CIP-007, R2.2 or create a mitigation plan.

Following data to provide breakdown of issues -

1. 62 CCA, EACM - Failed to track patches (R1.1)
2. 52 CCA EACM - Patch review conducted beyond 35 days (R1.2)
3. 29 CCA and EACM - implementation was beyond 35 days (R1.3) - Max 50 days

[Attachments \(\)](#)

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

All assets were assessed and summary of any patch violation was provided to the FRCC staff.

[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:

1. Complete Patch review for all devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO & PS).
2. Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).



3. Update the procedure to include controls for the following:
- a. 31 Day patch review/assessment for applicability from the date of last patch assessment for all patch releases since last patch assessment.
  - b. 31 Day implementation or Mitigation starting from the date of completion of patch assessment.
  - c. Application inventory tracking to ensure that all applications are being tracked for patches and updates. (1/15/2018 - IS & TI)
4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy periodically by SMEs or managers and verified by compliance. (2/15/2018 - IS & TI)
5. Training of applicable employees on new process, tools, and internal controls
6. Root Cause Analysis to identify root cause of noncompliance
7. Activities necessary to correct the noncompliance.
8. Perform an extent of condition evaluation

#### 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:

2/15/2018

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

Milestone Pending

Complete Patch review for all devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO & PS).

Milestone Pending (Due: 11/15/2017)

Complete Patch review for applicability for all the devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO & PS).

Extent of condition review for all applicable assets

Milestone Pending (Due: 11/15/2017)

Review for other assets to assess any issues and Identify any additional deficiencies and communicate to FRCC.

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).

Milestone Pending (Due: 12/15/2017)

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).

Review procedure adequacy and complete RCA for the subject violations

Milestone Pending (Due: 12/15/2017)

Review procedure adequacy and complete RCA for the subject violations

Update the procedure to include controls that will limit future risk of violations

Milestone Pending (Due: 1/15/2018)

3. Update the procedure to include at the minimum controls for the following:

- a. 31 Day patch review/assessment for applicability from the date of last patch assessment for all patch releases since last patch assessment.
- b. 31 Day implementation or Mitigation starting from the date of completion of patch assessment.
- c. Application inventory tracking to ensure that all applications are being tracked for patches and updates. (1/15/2018 - IS & TI)

Acknowledgement of control changes by SME, Manager, and Director

Milestone Pending (Due: 2/15/2018)

Acknowledgement of control changes by SME, Manager, and Directors or training for all SME impacted by this violations

#### 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):

These assets are behind a firewall and are protected using multi factor authentication. Remote access is closely monitored and any suspicious activity is alerted and responded.

#### Attachments ()

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

██████ determined that this violation resulted in Medium risk and after the completion, proper controls will be in place that will limit repetition of this violation.

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

## SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/18/2018

This item was marked ready for signature by [REDACTED] on 6/15/2018

## MEMBER MITIGATION PLAN EXTENSION

## SECTION A: REGISTERED ENTITY MITIGATION PLAN INFORMATION

Entity Name:

[REDACTED]

Standard:

CIP-007-6

Requirement ID(s):

R2.

NERC Violation ID(s):

FRCC2017017375

Original Mitigation Plan Expected Completion Date:

2/15/2018

## SECTION B: EXTENSION REQUEST REQUIREMENTS

Proposed Mitigation Plan Completion Date (must occur after 02/15/2018):

7/13/2018

Identify the reason an extension is being requested:

After realizing the extent of correcting the possible violations, [REDACTED] senior leadership decided to make an organizational change to create an independent position of Manager IT Assurance, with the primary purpose of reviewing and verifying compliance for the various periodic performance requirements in CIP (access revocation, patch review, patch implementation, monthly baseline monitoring, etc.). While the process is being undertaken to prevent new violation from occurring. For instance, patch reviews will now be performed and documented by the SME's, then by the SME's manager and before the 35 day window expires they will be reviewed by the Manager IT Assurance. This will allow for collection of information on problems with process, personnel, and tools while there is still time to make corrections before the time elapses. The new position became effective on 5/7/2018. The mitigation plan extension request is required for the new Manager to review and assess all corrective action plans required to complete all mitigations and milestones.

Provide detailed information as to why the original completion date will not be met:

After realizing the extent of correcting the possible violations, [REDACTED] senior leadership decided to make an organizational change to create an independent position of Manager IT Assurance, with the primary purpose of reviewing and verifying compliance for the various periodic performance requirements in CIP (access revocation, patch review, patch implementation, monthly baseline monitoring, etc.). While the process is being undertaken to prevent new violation from occurring. For instance, patch reviews will now be performed and documented by the SME's, then by the SME's manager and before the 35 day window expires they will be reviewed by the Manager IT Assurance. This will allow for collection of information on problems with process, personnel, and tools while there is still time to make corrections before the time elapses. The new position became effective on 5/7/2018. The mitigation plan extension request is required for the new Manager to review and assess all corrective action plans required to complete all mitigations and milestones.

## SECTION D.3: MILESTONE ACTIVITY

Milestone Pending

[Complete Patch review for all devices to include all patches released till date for all devices determined as non-compliant for this SR \(11/15/2017 - IS, TI, BPO & PS\).](#)

Milestone Pending (Due: 11/15/2017)

Complete Patch review for applicability for all the devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO &amp; PS).

[Extent of condition review for all applicable assets](#)

Milestone Completed (Due: 11/15/2017 and Completed 9/28/2017)

Review for other assets to assess any issues and Identify any additional deficiencies and communicate to FRCC.

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

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS)

Milestone Pending (Due: 12/15/2017)

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).

Review procedure adequacy and complete RCA for the subject violations

Milestone Completed (Due: 12/15/2017 and Completed 4/14/2018)

Review procedure adequacy and complete RCA for the subject violations

Update the procedure to include controls that will limit future risk of violations

Milestone Completed (Due: 1/15/2018 and Completed 1/22/2018)

3. Update the procedure to include at the minimum controls for the following:

- a. 31 Day patch review/assessment for applicability from the date of last patch assessment for all patch releases since last patch assessment.
- b. 31 Day implementation or Mitigation starting from the date of completion of patch assessment.
- C. Application inventory tracking to ensure that all applications are being tracked for patches and updates. (1/15/2018 - IS & TI)

Acknowledgement of control changes by SME, Manager, and Director

Milestone Completed (Due: 2/15/2018 and Completed 1/31/2018)

Acknowledgement of control changes by SME, Manager, and Directors or training for all SME impacted by this violations



This item was signed by [REDACTED] on 7/19/2018

This item was marked ready for signature by Miles Albritton (malbritton@frcc.com) on 7/19/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-007-6

Requirement	Tracking Number	NERC Violation ID
R2.	FRCC2017-100923	FRCC2017017375

Date of completion of the Mitigation Plan:

7/13/2018

Extent of condition review for all applicable assets

Milestone Completed (Due: 11/15/2017 and Completed 9/28/2017)

[Attachments \(0\)](#)

Review for other assets to assess any issues and Identify any additional deficiencies and communicate to FRCC.

Review procedure adequacy and complete RCA for the subject violations

Milestone Completed (Due: 12/15/2017 and Completed 3/14/2018)

[Attachments \(0\)](#)

Review procedure adequacy and complete RCA for the subject violations

Update the procedure to include controls that will limit future risk of violations

Milestone Completed (Due: 1/15/2018 and Completed 1/22/2018)

[Attachments \(0\)](#)

3. Update the procedure to include at the minimum controls for the following:

- 31 Day patch review/assessment for applicability from the date of last patch assessment for all patch releases since last patch assessment.
- 31 Day implementation or Mitigation starting from the date of completion of patch assessment.
- C. Application inventory tracking to ensure that all applications are being tracked for patches and updates. (1/15/2018 - IS & TI)

Acknowledgement of control changes by SME, Manager, and Director

Milestone Completed (Due: 2/15/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

Acknowledgement of control changes by SME, Manager, and Directors or training for all SME impacted by this violations

Complete Patch review for all devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO & PS).

Milestone Completed (Due: 6/30/2018 and Completed 6/30/2018)

[Attachments \(0\)](#)

Complete Patch review for applicability for all the devices to include all patches released till date for all devices determined as non-compliant for this SR (11/15/2017 - IS, TI, BPO & PS).

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).

Milestone Completed (Due: 7/13/2018 and Completed 7/13/2018)

[Attachments \(0\)](#)

Implement Patches that are assessed as applicable in step 1 or create Mitigation Plan. (11/15/2017 - TS, BPO & PS).

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

[REDACTED] will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

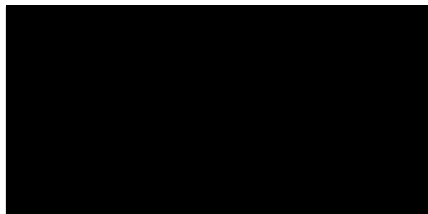


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 27, 2018



Re: [REDACTED] ( [REDACTED] )  
**Mitigation Plan Verification of Completion**  
**FRCC2017017375 (CIP-007-6 R2)**

Dear [REDACTED]

The Mitigation Plan Certification of Completion submitted by [REDACTED] ( [REDACTED] ) for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017375	CIP-007-6 R2	July 19, 2018

After review for completion on **September 24, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma



## Attachment 8

- 8a. The Entity's Mitigation Plan designated as FRCCMIT013383 for CIP-007-6 R4 submitted November 9, 2017;
- 8b. The Entity's Request for Mitigation Plan Extension for CIP-007-6 R4 submitted June 18, 2018;
- 8c. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R4 submitted July 12, 2018;
- 8d. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R4 dated September 13, 2018;

This item was signed by [REDACTED] on 11/9/2017

This item was marked ready for signature by [REDACTED] on 10/22/2017

## SECTION A: COMPLIANCE NOTICES &amp; MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

## B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]  
[REDACTED]

Compliance Registry ID: [REDACTED]

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

Name: [REDACTED]

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

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

Standard:

CIP-007-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R4.	FRCC2017-100935	FRCC2017017833	[REDACTED]

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

[REDACTED] self reported that it failed to log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

1. Detected successful login attempts;
2. Detected failed access attempts and failed login attempts;

Devices that were impacted by this violations included 5 PACS systems. [REDACTED] 3 servers , logging was impacted for 3 days and [REDACTED] was impacted for 15 days.

[REDACTED] did not log all the security events for 17 BCA workstations as required by CIP-007, R4, for the audit period.

[Attachments \(\)](#)

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

Logging failures were caused by bad configurations.

[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:

1. Correct logging configurations and verify for compliance for all requirements of CIP-007, R4.(11/15/2017 - IS)
2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)
3. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS & TI)

#### 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:

1/31/2018

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

#### Perform Root Cause Analysis for logging issues

Milestone Pending (Due: 10/10/2017)

Perform Root Cause analysis and determine changes required to existing controls.

#### Perform Extent of condition review

Milestone Pending (Due: 10/16/2017)

Review other system where logging configuration issues may exist.

#### 1. Correct logging configurations and verify for compliance for all requirements of CIP-007, R4.(11/15/2017 - IS)

Milestone Pending (Due: 11/15/2017)

Many logging issues that resulted from bad configurations were fixed, but many others are going through review and will be fixed as per milestone 1.

#### 2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)

Milestone Pending (Due: 12/15/2017)

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)

This milestone is to ensure that all new devices are being configured for proper logging configurations.

#### 3. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS & TI)

Milestone Pending (Due: 1/15/2018)

This milestone is to ensure configuration is being performed correctly and SMEs are accountable for the completion of the tasks.

#### Training or Acknowledgement for impacted SME where controls have been updated.

Milestone Pending (Due: 1/31/2018)

If this subject can be included in training, else a direct certification of understanding will be sought from the SMEs

### 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):

██████████ is continually monitoring the logs and while some correction are still being planned, many have already been corrected.

#### Attachments ()

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

Milestone 2 and 3 are designed to limit any future risk of violations.

#### 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 FRCC 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 ██████████ of ██████████

- I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
- I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/18/2018

This item was marked ready for signature by [REDACTED] on 6/15/2018

## MEMBER MITIGATION PLAN EXTENSION

## SECTION A: REGISTERED ENTITY MITIGATION PLAN INFORMATION

Entity Name:

[REDACTED]

Standard:

CIP-007-6

Requirement ID(s):

R4.

NERC Violation ID(s):

FRCC2017017833

Original Mitigation Plan Expected Completion Date:

1/31/2018

## SECTION B: EXTENSION REQUEST REQUIREMENTS

Proposed Mitigation Plan Completion Date (must occur after 01/31/2018):

4/18/2018

Identify the reason an extension is being requested:

After realizing the extent of correcting the possible violations, [REDACTED] senior leadership decided to make an organizational change to create an independent position of Manager IT Assurance, with the primary purpose of reviewing and verifying compliance for the various periodic performance requirements in CIP (access revocation, patch review, patch implementation, monthly baseline monitoring, etc.). While the process is being undertaken to prevent new violation from occurring. For instance, patch reviews will now be performed and documented by the SME's, then by the SME's manager and before the 35 day window expires they will be reviewed by the Manager IT Assurance. This will allow for collection of information on problems with process, personnel, and tools while there is still time to make corrections before the time elapses. The new position became effective on 5/7/2018. The mitigation plan extension request is required for the new Manager to review and assess all corrective action plans required to complete all mitigations and milestones.

Provide detailed information as to why the original completion date will not be met:

After realizing the extent of correcting the possible violations, [REDACTED] senior leadership decided to make an organizational change to create an independent position of Manager IT Assurance, with the primary purpose of reviewing and verifying compliance for the various periodic performance requirements in CIP (access revocation, patch review, patch implementation, monthly baseline monitoring, etc.). While the process is being undertaken to prevent new violation from occurring. For instance, patch reviews will now be performed and documented by the SME's, then by the SME's manager and before the 35 day window expires they will be reviewed by the Manager IT Assurance. This will allow for collection of information on problems with process, personnel, and tools while there is still time to make corrections before the time elapses. The new position became effective on 5/7/2018. The mitigation plan extension request is required for the new Manager to review and assess all corrective action plans required to complete all mitigations and milestones.

## SECTION D.3: MILESTONE ACTIVITY

[Perform Root Cause Analysis for logging issues](#)

Milestone Completed (Due: 10/10/2017 and Completed 1/4/2018)

Perform Root Cause analysis and determine changes required to existing controls.

[Perform Extent of condition review](#)

Milestone Completed (Due: 10/16/2017 and Completed 9/28/2017)

Review other system where logging configuration issues may exist.

[1. Correct logging configurations and verify for compliance for all requirements of CIP-007, R4.\(11/15/2017 - IS\)](#)

Milestone Completed (Due: 11/15/2017 and Completed 4/18/2018)



Many logging issues that resulted from bad configurations were fixed, but many others are going through review and will be fixed as per milestone 1.

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)

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

Milestone Completed (Due: 12/15/2017 and Completed 1/23/2018)

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)

This milestone is to ensure that all new devices are being configured for proper logging configurations.

3. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS & TI)

Milestone Completed (Due: 1/15/2018 and Completed 1/22/2018)

This milestone is to ensure configuration is being performed correctly and SMEs are accountable for the completion of the tasks.

Training or Acknowledgement for impacted SME where controls have been updated.

Milestone Completed (Due: 1/31/2018 and Completed 1/31/2018)

If this subject can be included in training, else a direct certification of understanding will be sought from the SMEs

This item was signed by [REDACTED] on 7/12/2018

This item was marked ready for signature by [REDACTED] on 7/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-007-6

Requirement	Tracking Number	NERC Violation ID
R4.	FRCC2017-100935	FRCC2017017833

Date of completion of the Mitigation Plan:

4/18/2018

Perform Root Cause Analysis for logging issues

Milestone Completed (Due: 10/10/2017 and Completed 1/4/2018)

[Attachments \(0\)](#)

Perform Root Cause analysis and determine changes required to existing controls.

Perform Extent of condition review

Milestone Completed (Due: 10/16/2017 and Completed 9/28/2017)

[Attachments \(0\)](#)

Review other system where logging configuration issues may exist.

1. Correct logging configurations and verify for compliance for all requirements of CIP-007, R4.(11/15/2017 - IS)

Milestone Completed (Due: 11/15/2017 and Completed 4/18/2018)

[Attachments \(0\)](#)

Many logging issues that resulted from bad configurations were fixed, but many others are going through review and will be fixed as per milestone 1.

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS & TI)

Milestone Completed (Due: 12/15/2017 and Completed 1/23/2018)

[Attachments \(0\)](#)

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Manager Sign-offs (12/15/2017 - IS &amp; TI)

This milestone is to ensure that all new devices are being configured for proper logging configurations.

3. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS & TI)

Milestone Completed (Due: 1/15/2018 and Completed 1/22/2018)

[Attachments \(0\)](#)

This milestone is to ensure configuration is being performed correctly and SMEs are accountable for the completion of the tasks.

Training or Acknowledgement for impacted SME where controls have been updated.

Milestone Completed (Due: 1/31/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

If this subject can be included in training, else a direct certification of understanding will be sought from the SMEs

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

[REDACTED] will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

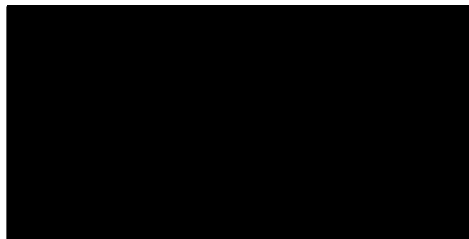


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 13, 2018



Re: [REDACTED]  
**Mitigation Plan Verification of Completion  
FRCC2017017833 (CIP-007-6 R4)**

Dear [REDACTED],

The Mitigation Plan Certification of Completion submitted by [REDACTED] for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017833	CIP-007-6 R4	July 12, 2018

After review for completion on **September 12, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma



## Attachment 9

- 9a. The Entity's Mitigation Plan designated as FRCCMIT013382 for CIP-007-6 R5 submitted November 16, 2017;
- 9b. The Entity's Certification of Mitigation Plan Completion for CIP-007-6 R5 submitted July 18, 2018;
- 9c. FRCC's Verification of Mitigation Plan Completion for CIP-007-6 R5 dated September 13, 2018;

This item was signed by [REDACTED] on 11/16/2017

This item was marked ready for signature by [REDACTED] on 11/13/2017

## SECTION A: COMPLIANCE NOTICES &amp; MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

## B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]  
[REDACTED]

Compliance Registry ID: [REDACTED]

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

Name: [REDACTED]

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

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

Standard:

CIP-007-6

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R5.	FRCC2017-100938	FRCC2017017857	[REDACTED]

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

[REDACTED] is self Report CIP-007 R5.7 because it failed to implement controls to Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts for [REDACTED] SIEM devices including the following devices -

7 SIEM devices and 4 domain controllers

[Attachments \(0\)](#)

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

4 Domain Controllers were identified as part of extent of condition review.

[Attachments \(0\)](#)

## 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:

Correct the misconfiguration for subject devices to lock account after 5 consecutive failed attempts and alert for response (pending - Immediate action required).(11/15/2017 - IS)

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/15/2018 - IS)

Update MD-202 to enable requirement that all [REDACTED] security devices where technically and operationally feasible must be configured to their highest ability, even if that is beyond the requirements of CIP Standards. (11/15/2017 - Comp)

Training of applicable employees on new process, tools, and internal controls

Root Cause Analysis to identify root cause of noncompliance

Perform an extent of condition evaluation

#### 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:

2/15/2018

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

#### Complete Extent of condition review

Milestone Pending (Due: 11/15/2017)

After discovery of this violation, [REDACTED] will complete a review of this violation to confirm if there are other devices with similar misconfigurations.

#### Complete a Root Cause Assessment

Milestone Pending (Due: 11/15/2017)

Complete a Root Cause Assessment

#### Update MD-202 to enable requirement that all [REDACTED] security devices

Milestone Pending (Due: 11/15/2017)

Update MD-202 to enable requirement that all [REDACTED] security devices where technically and operationally feasible must be configured to their highest ability, even if that is beyond the requirements of CIP Standards. (11/15/2017 - Comp)

#### Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables

Milestone Pending (Due: 1/15/2018)

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/15/2018 - IS)

#### Training of applicable employees on new process, tools, and internal controls or acknowledgement of understanding

Milestone Pending (Due: 2/15/2018)

Training of applicable employees on new process, tools, and internal controls or acknowledgement of understanding

### 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):

[REDACTED] agrees that this violation potential risk was not minimal but moderate because lack of this control will allow unauthorized person unlimited opportunity attempts to compromise the password controls. However, [REDACTED] corporate controls may minimize any access to these devices.

#### Attachments ()

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

[REDACTED] is modifying controls for implementation of new devices and also updating the policy to address such potential violations.

#### 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 FRCC 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]
  - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
  - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
  - I have read and am familiar with the contents of this Mitigation Plan

- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

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

#### SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 7/18/2018

This item was marked ready for signature by [REDACTED] on 7/17/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-007-6

Requirement	Tracking Number	NERC Violation ID
R5.	FRCC2017-100938	FRCC2017017857

Date of completion of the Mitigation Plan:

2/15/2018

[Complete Extent of condition review](#)

Milestone Completed (Due: 11/15/2017 and Completed 9/28/2017)

[Attachments \(0\)](#)

After discovery of this violation, [REDACTED] will complete a review of this violation to confirm if there are other devices with similar misconfigurations.

[Complete a Root Cause Assessment](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Complete a Root Cause Assessment

[Update MD-202 to enable requirement that all \[REDACTED\] security devices](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Update MD-202 to enable requirement that all [REDACTED] security devices where technically and operationally feasible must be configured to their highest ability, even if that is beyond the requirements of CIP Standards. (11/15/2017 - Comp)

[Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/15/2018 - IS)

[Training of applicable employees on new process, tools, and internal controls or acknowledgement of understanding](#)

Milestone Completed (Due: 2/15/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

Training of applicable employees on new process, tools, and internal controls or acknowledgement of understanding

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

[REDACTED] will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

[REDACTED] will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

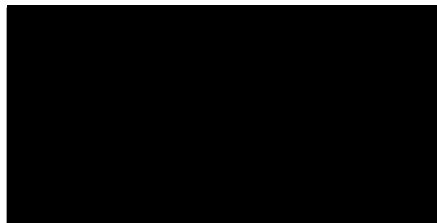


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 13, 2018



Re: [REDACTED]  
**Mitigation Plan Verification of Completion  
FRCC2017017857 (CIP-007-6 R5)**

Dear [REDACTED],

The Mitigation Plan Certification of Completion submitted by [REDACTED] for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017857	CIP-007-6 R5	July 18, 2018

After review for completion on **September 12, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 10

- 10a. The Entity's Mitigation Plan designated as FRCCMIT013374 for CIP-010-2 R1 submitted November 9, 2017;
- 10b. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R1 submitted July 18, 2018;
- 10c. FRCC's Verification of Mitigation Plan Completion for CIP-010-2 R1 dated September 11, 2018;



 A [previous version](#) of this Mitigation Plan exists



 This item was signed by [REDACTED] on 11/9/2017



 This item was marked ready for signature by [REDACTED] on 11/7/2017



## SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

### B.1 Identify your organization

Company Name:

[REDACTED]

Company Address:

[REDACTED]

[REDACTED]

Compliance Registry ID:

[REDACTED]

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

Name:

[REDACTED]

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

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

Standard:

CIP-010-2

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	FRCC2017-100922	FRCC2017017376	[REDACTED]

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

[REDACTED] self reported this violation in abundance of caution as it's not very clear whether the IPS embedded modules with it's own distinct baselines should be identified as separate Cyber Assets and individually classified as EACM. [REDACTED] failed to develop baseline as required by CIP-010, R1.1. During compliance review it was determined that [REDACTED] SMEs failed to develop baseline configurations for 5 devices. [REDACTED] installed new IPS modules in the Firewalls, but due to misunderstanding, did not consider IPS modules as separate cyber asset. It was determined that IPS modules have completely different baselines (OS, Ports, Accounts, Configuration Management etc.). Root cause of this violation could also be attributed to the fact that device changes were made prior to CIP Version 5 enforcement date of April 1, 2015, when creating baselines were not required.

[Attachments \(\)](#)

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

During the audit period as a result of extent of condition review, additional devices were identified and report submitted to the FRCC.

[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:

1. Asset Owner correct and approve Baselines. Complete verification by compliance department (11/15/2017 - Comp, IS, TI, BPO & PS).
2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/15/2018 - IS & TI)
3. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (2/1/2018 - IS & TI)

4. Training of applicable employees on new process, tools, and internal controls - 2/15/2018
5. Root Cause Analysis to identify root cause of noncompliance
6. Perform an extent of condition evaluation

NON-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:

2/15/2018

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

Asset Owner correct and approve Baselines. Complete verification by compliance department (11/15/2017 - Comp. IS, TI, BPO & PS).

Milestone Pending (Due: 11/15/2017)

1. Asset Owner correct and approve Baselines. Complete verification by compliance department (11/15/2017 - Comp. IS, TI, BPO & PS).

Complete extent of condition review, document additional issues if identified and submit scope of expansion form

Milestone Pending (Due: 11/30/2017)

Complete extent of condition review, document additional issues if identified and submit scope of expansion form

Complete Root Cause Analysis for identified issues

Milestone Pending (Due: 12/1/2017)

Complete Root Cause Analysis for identified issues

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/30/2018 - IS & TI)

Milestone Pending (Due: 1/15/2018)

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/30/2018 - IS & TI)

Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (2/1/2018 - IS & TI)

Milestone Pending (Due: 2/1/2018)

Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (2/1/2018 - IS & TI)

Complete Training for new controls or complete acknowledgement of understanding of new controls from impacted SMEs.

Milestone Pending (Due: 2/15/2018)

Complete Training for new controls or complete acknowledgement of understanding of new controls from impacted SMEs.

#### 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):

For the interim period [REDACTED] has implemented security controls as these devices are closely monitored and behind the corporate security enclosure and hence limit the exposure.

#### Attachments ()

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

[REDACTED] is implementing controls to ensure that the risk of such violation happening in future is limited. Mitigation plan includes such steps.

#### 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 FRCC 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]
- I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
- I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
- I have read and am familiar with the contents of this Mitigation Plan
- [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

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

#### SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 7/18/2018

This item was marked ready for signature by [REDACTED] on 7/17/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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):

CIP-010-2

Requirement	Tracking Number	NERC Violation ID
R1.	FRCC2017-100922	FRCC2017017376

Date of completion of the Mitigation Plan:

2/15/2018

[Asset Owner correct and approve Baselines. Complete verification by compliance department \(11/15/2017 - Comp, IS, TI, BPO & PS\).](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

1. Asset Owner correct and approve Baselines. Complete verification by compliance department (11/15/2017 - Comp, IS, TI, BPO &amp; PS).

[Complete extent of condition review, document additional issues if identified and submit scope of expansion form](#)

Milestone Completed (Due: 11/30/2017 and Completed 9/28/2017)

[Attachments \(0\)](#)

Complete extent of condition review, document additional issues if identified and submit scope of expansion form

[Complete Root Cause Analysis for identified issues](#)

Milestone Completed (Due: 12/1/2017 and Completed 12/1/2017)

[Attachments \(0\)](#)

Complete Root Cause Analysis for identified issues

[Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. \(1/30/2018 - IS & TI\)](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (1/30/2018 - IS &amp; TI)

[Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. \(2/1/2018 - IS & TI\)](#)

Milestone Completed (Due: 2/1/2018 and Completed 1/22/2018)

[Attachments \(0\)](#)

Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (2/1/2018 - IS &amp; TI)

[Complete Training for new controls or complete acknowledgement of understanding of new controls from impacted SMEs.](#)

Milestone Completed (Due: 2/15/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

Complete Training for new controls or complete acknowledgement of understanding of new controls from impacted SMEs.

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

[REDACTED] will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans



Description of the information provided to FRCC for their evaluation \*

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

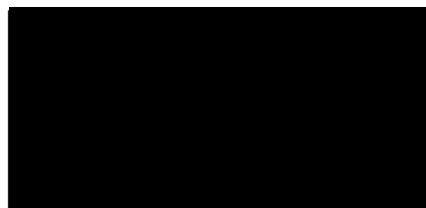


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 11, 2018



Re:



**Mitigation Plan Verification of Completion  
FRCC2017017376 (CIP-010-2 R1)**

Dear [REDACTED],

The Mitigation Plan Certification of Completion submitted by [REDACTED] for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017376	CIP-010-2 R1	July 18, 2018

After review for completion on **September 11, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.


Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 11

- 11a. The Entity's Mitigation Plan designated as FRCCMIT013370 for CIP-010-2 R3 submitted November 9, 2017;
- 11b. The Entity's Certification of Mitigation Plan Completion for CIP-010-2 R3 submitted June 12, 2018;
- 11c. FRCC's Verification of Mitigation Plan Completion for CIP-010-2 R3 dated September 24, 2018;

 A [previous version](#) of this Mitigation Plan exists



 This item was signed by [REDACTED] on 11/9/2017



 This item was marked ready for signature by [REDACTED] on 10/30/2017



## SECTION A: COMPLIANCE NOTICES & MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

### B.1 Identify your organization

Company Name:

[REDACTED]

Company Address:

[REDACTED]

[REDACTED]

Compliance Registry ID:

[REDACTED]

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

Name:

[REDACTED]

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

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

Standard:

CIP-010-2

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R3.	FRCC2017-100937	FRCC2017017835	[REDACTED]

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

[REDACTED] self Reported that it failed to perform an active vulnerability assessment of two new Cyber Assets, prior to adding them to the production environment as a Protected Cyber Assets (PCA). Two switches, were placed in production and [REDACTED] completed the active CVA on June 27, 2017 instead of 12/1/2016, when they were placed in service. Further review for extent of condition did not find any other violation.

[Attachments \(\)](#)

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

These two devices are not BCA but PCA and lack of proper control may have resulted in this violation.

[Attachments \(\)](#)

## SECTION D: DETAILS OF PROPOSED MITIGATION PLAN

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

1. Perform required Vulnerability Assessment and complete review by Compliance (12/31/2016 - Complete).
2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (12/15/2017 - IS)
3. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2017 - IS)



4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS, TI, BPO)
5. Training of applicable employees on new process, tools, and internal controls
6. Root Cause Analysis to identify root cause of noncompliance
7. Perform an extent of condition evaluation

NON-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:

1/15/2018

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

#### Complete active CVA for two subject devices

Milestone Pending (Due: 12/30/2016)

Complete active CVA for two subject devices

#### 5. Perform Extent of condition review

Milestone Pending (Due: 11/15/2017)

5. Perform Extent of condition review

#### 2. Document controls for review process for all New assets

Milestone Pending (Due: 12/15/2017)

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (12/15/2017 - IS)

a. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2018 - IS)

#### 3. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2017 - IS)

Milestone Pending (Due: 12/15/2017)

3. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2017 - IS)

#### 4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS, TI, BPO)

Milestone Pending (Due: 1/15/2018)

4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS, TI, BPO)

#### Training or attestation / acknowledgement for SME confirming their understanding of new controls

Milestone Pending (Due: 1/15/2018)

Training or attestation / acknowledgement for SME confirming their understanding of new controls

#### 7. Root Cause Analysis to identify root cause of noncompliance and any corrective measure if needed

Milestone Pending (Due: 1/15/2018)

7. Root Cause Analysis to identify root cause of noncompliance and any corrective measure if needed

### 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):

These devices were PCA which were well protected behind the ESP protective measures. Further the violation was limited to a very short period of less than 15 days of deployment.

#### Attachments ()

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

additional controls designed for the mitigation will prompt SME for requirement of CVA for new devices and further, we have added that a Director level accountability control to be performed.

## 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 FRCC 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]
  - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
  - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
  - I have read and am familiar with the contents of this Mitigation Plan
  - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

## SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com



This item was signed by [REDACTED] on 6/12/2018

This item was marked ready for signature by [REDACTED] on 6/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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:

Name of Standard of mitigation violation(s):

CIP-010-2

Requirement	Tracking Number	NERC Violation ID
R3.	FRCC2017-100937	FRCC2017017835

Date of completion of the Mitigation Plan:

1/15/2018

[Complete active CVA for two subject devices](#)

Milestone Completed (Due: 12/30/2016 and Completed 12/30/2016)

[Attachments \(0\)](#)

Complete active CVA for two subject devices

[5. Perform Extent of condition review](#)

Milestone Completed (Due: 11/15/2017 and Completed 6/9/2017)

[Attachments \(0\)](#)

5. Perform Extent of condition review

[2. Document controls for review process for all New assets](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

2. Document controls for review process for all New assets to ensure that evidence meets required minimum deliverables, such as completed Check List, Testing results output, Completed and approved baseline, Manager Sign-offs. (12/15/2017 - IS)

a. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2018 - IS)

[3. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification \(12/15/2017 - IS\)](#)

Milestone Completed (Due: 12/15/2017 and Completed 12/15/2017)

[Attachments \(0\)](#)

3. Update Procedure and controls to ensure that all new assets implementation includes Security Assessment Scan and documented results are stored for compliance verification (12/15/2017 - IS)

[4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. \(1/15/2018 - IS, TI, BPO\)](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

4. Document and Implement controls to ensure that all supporting evidence is stored and reviewed for accuracy prior to completion of testing ticket by SME peers or managers and verified by compliance. (1/15/2018 - IS, TI, BPO)

[Training or attestation / acknowledgement for SME confirming their understanding of new controls](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/15/2018)

[Attachments \(0\)](#)

Training or attestation / acknowledgement for SME confirming their understanding of new controls

[7. Root Cause Analysis to identify root cause of noncompliance and any corrective measure if needed](#)

Milestone Completed (Due: 1/15/2018 and Completed 1/4/2018)

7. Root Cause Analysis to identify root cause of noncompliance and any corrective measure if needed

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

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

will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.



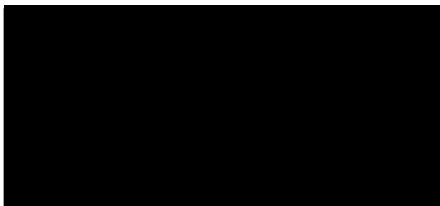


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 24, 2018



Re:



**Mitigation Plan Verification of Completion  
FRCC2017017835 (CIP-010-2 R3)**

Dear



The Mitigation Plan Certification of Completion submitted by [REDACTED] for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017835	CIP-010-2 R3	June 12, 2018

After review for completion on **September 21, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.




Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma

## Attachment 12

- 12a. The Entity's Mitigation Plan designated as FRCCMIT013373 for CIP-011-2 R1 submitted November 9, 2017;
- 12b. The Entity's Certification of Mitigation Plan Completion for CIP-011-2 R1 submitted June 12, 2018;
- 12c. FRCC's Verification of Mitigation Plan Completion for CIP-011-2 R1 dated September 11, 2018.

 A [previous version](#) of this Mitigation Plan exists This item was signed by [REDACTED] on 11/9/2017 This item was marked ready for signature by [REDACTED] on 11/6/2017

## SECTION A: COMPLIANCE NOTICES &amp; MITIGATION PLAN REQUIREMENTS

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

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

## SECTION B: REGISTERED ENTITY INFORMATION

## B.1 Identify your organization

Company Name: [REDACTED]

Company Address: [REDACTED]  
[REDACTED]

Compliance Registry ID: [REDACTED]

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

Name: [REDACTED]

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

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

Standard:

CIP-011-2

Requirement	Regional ID	NERC Violation ID	Date Issue Reported
R1.	FRCC2017-100929	FRCC2017017696	[REDACTED]

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

[REDACTED] self reported that it failed to identify all storage locations that included It's BES Cyber System Information. It was determined by [REDACTED] compliance team that [REDACTED] and [REDACTED] servers and [REDACTED] system were not identified as locations of BCSl. These devices to store information that is classified as BCSl. These devices were identified on May 11, 2017, and not by the enforcement date of July 01, 2016 as required by the Standard. [REDACTED] is reporting these for lack of sufficient documentation to demonstrate compliance that these locations were identified as BCSl location as required on July 1, 2016.

[Attachments \(\)](#)

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

While these devices may not have been identified, sufficient protection was in place and potential risk was minimal.

[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:

1. Update list of all Cyber Assets that contain BCSl (Complete - 07/01/2017).
2. Perform compliance review and implement required security controls (11/30/2017 - IS).
3. Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp?).
4. Create and Implement Formal BCSl asset identification process, including deliverables such as Survey submitted to all SME department heads annually (1/10/2018 -



- IS).
5. Create and Implement controls for annual review and independent review by compliance department (1/25/2018 - IS).
  6. Create controls and implement in Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied. (2/15/2018 - IS).
  7. Training of applicable employees on new process, tools, and internal controls
  8. Root Cause Analysis to identify root cause of noncompliance
  9. Activities necessary to correct the noncompliance.
  10. Perform an extent of condition evaluation
- NON-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:

2/15/2018

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

Update list of all Cyber Assets that contain BCSI (Complete - 07/01/2017).

Milestone Pending (Due: 7/1/2017)

Update list of all Cyber Assets that contain BCSI (Complete - 07/01/2017).

Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp).

Milestone Pending (Due: 11/15/2017)

Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp).

Perform Root cause analysis to identify the cause of violation.

Milestone Pending (Due: 11/15/2017)

Perform Root cause analysis to identify the cause of violation.

Perform compliance review and implement required security controls (11/30/2017 - IS).

Milestone Pending (Due: 11/30/2017)

Perform compliance review and implement required security controls (11/30/2017 - IS).

Perform Extent of condition review

Milestone Pending (Due: 11/30/2017)

Perform Extent of condition review for BCSI viola ion

Create and Implement Formal BCSI asset identification process, including deliverables such as Survey submitted to all SME department heads annually (1/10/2018 - IS).

Milestone Pending (Due: 1/10/2018)

Create and Implement Formal BCSI asset identification process, including deliverables such as Survey submitted to all SME department heads annually (1/10/2018 - IS).

Create controls and implement in Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied. (2/15/2018 - IS).

Milestone Pending (Due: 2/15/2018)

6. Create controls and implement in Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied. (2/15/2018 - IS).

Train SME on new controls or confirm their acknowledgement of understanding

Milestone Pending (Due: 2/15/2018)

Train SME on new controls or confirm their acknowledgement of understanding

#### 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):

As stated earlier, these systems are well protected by [REDACTED] corporate infrastructure and only authorized access is allowed. Risk to the systems was minimal and mostly originated from lack of documentation.

#### Attachments ()

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

Three milestones were added to include process and controls that will limit risk of future violations, including a documented process for identifying BCSI assets, controls to implement BCSI assets implementation at the provisioning control.



## 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 FRCC 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]
  - I am qualified to sign this Mitigation Plan on behalf of [REDACTED]
  - I understand [REDACTED] obligations to comply with Mitigation Plan requirements and ERO remedial action directives as well as ERO documents, including, but not limited to, the NERC Rules of Procedure, including Appendix 4 (Compliance Monitoring and Enforcement Program of the North American Electric Reliability Corporation (NERC CMEP))
  - I have read and am familiar with the contents of this Mitigation Plan
  - [REDACTED] agrees to comply with, this Mitigation Plan, including the timetable completion date, as accepted by FRCC and approved by NERC

## SECTION G: REGIONAL ENTITY CONTACT

Please direct any questions regarding completion of this form to:

Your assigned Risk Assessment and Mitigation Plan (RAM) Specialist single point of contact (SPOC).

If you do not know your assigned RAM Specialist, please contact the FRCC Compliance Risk Assessment and Mitigation department to determine your assigned SPOC at:

FRCC Compliance – Risk Assessment and Mitigation

(813) 289-5644

FRCCComplianceRAM@frcc.com

This item was signed by [REDACTED] on 6/12/2018

This item was marked ready for signature by [REDACTED] on 6/12/2018

## MEMBER MITIGATION PLAN CLOSURE

All Mitigation Plan Completion Certification submittals shall include data or information sufficient for FRCC to verify completion of the Mitigation Plan. FRCC 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:

Name of Standard of mitigation violation(s):

CIP-011-2

Requirement	Tracking Number	NERC Violation ID
R1.	FRCC2017-100929	FRCC2017017696

Date of completion of the Mitigation Plan:

2/15/2018

[Update list of all Cyber Assets that contain BCSI \(Complete - 07/01/2017\).](#)

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

[Attachments \(0\)](#)

Update list of all Cyber Assets that contain BCSI (Complete - 07/01/2017).

[Revise CIP Policy \(MD-202\) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. \(11/15/2017 - Comp\).](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Revise CIP Policy (MD-202) to add requirements for SME Compliance Responsibilities and specify process and ownership for resolution of Compliance Interpretations. (11/15/2017 - Comp).

[Perform Root cause analysis to identify the cause of violation.](#)

Milestone Completed (Due: 11/15/2017 and Completed 11/15/2017)

[Attachments \(0\)](#)

Perform Root cause analysis to identify the cause of violation.

[Perform compliance review and implement required security controls \(11/30/2017 - IS\).](#)

Milestone Completed (Due: 11/30/2017 and Completed 11/30/2017)

[Attachments \(0\)](#)

Perform compliance review and implement required security controls (11/30/2017 - IS).

[Perform Extent of condition review](#)

Milestone Completed (Due: 11/30/2017 and Completed 7/24/2017)

[Attachments \(0\)](#)

Perform Extent of condition review for BCSI violation

[Create and Implement Formal BCSI asset identification process, including deliverables such as Survey submitted to all SME department heads annually \(1/10/2018 - IS\).](#)

Milestone Completed (Due: 1/10/2018 and Completed 1/10/2018)

[Attachments \(0\)](#)

Create and Implement Formal BCSI asset identification process, including deliverables such as Survey submitted to all SME department heads annually (1/10/2018 - IS).

[Create controls and implement in Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied. \(2/15/2018 - IS\).](#)

Milestone Completed (Due: 2/15/2018 and Completed 2/15/2018)

[Attachments \(0\)](#)

6. Create controls and implement in Identity Management system to ensure that BCSI assets are identified individually and CIP controls are applied. (2/15/2018 - IS).

[Train SME on new controls or confirm their acknowledgement of understanding](#)

Milestone Completed (Due: 2/15/2018 and Completed 1/31/2018)

[Attachments \(0\)](#)

Train SME on new controls or confirm their acknowledgement of understanding

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

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

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

Description of the information provided to FRCC for their evaluation \*

██████████ will provide a data narrative detailing the actions taken to complete the relevant mitigation and milestone plans

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.

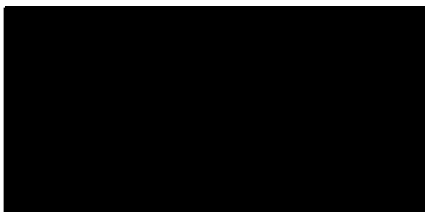


NON-PUBLIC AND CONFIDENTIAL INFORMATION  
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.  
3000 BAYPORT DRIVE, SUITE 600  
TAMPA, FLORIDA 33607-8410  
PHONE 813.289.5644 • FAX 813.289.5646  
WWW.FRCC.COM

**VIA Secure Folder and E-MAIL**

September 11, 2018



Re:



**Mitigation Plan Verification of Completion  
FRCC2017017696 (CIP-011-2 R1)**

Dear



The Mitigation Plan Certification of Completion submitted by [REDACTED] for the referenced violation has been received by the Florida Reliability Coordinating Council, Inc. (FRCC) on the specified date noted below.

Mitigation Plan	Standard / Requirement	Received On
FRCC2017017696	CIP-011-2 R1	June 12, 2018

After review for completion on **September 11, 2018**, FRCC Compliance staff finds that [REDACTED] has completed this Mitigation Plan. FRCC will notify NERC that [REDACTED] has completed this mitigation plan.

If you have any questions, please feel free to contact Miles Albritton at 813-605-5346.

Respectfully,

Chris Holmquest  
Manager of Risk Assessment and Mitigation  
[cholmquest@frcc.com](mailto:cholmquest@frcc.com)

CH/ma