A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

COVER PAGE

This filing contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the SNOPs in this filing and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	RFC2017018305	Yes		Yes	Yes	Yes	Yes		Yes					Category 1: 3 years; Category 2-
2	RFC2016016353	Yes		Yes	Yes		Yes				Yes			12: 2 years.
3	RFC2017018475	Yes		Yes	Yes		Yes							Category 1: 3 years; Category 2-
4	RFC2018019404	Yes		Yes	Yes		Yes		Yes	Yes				12: 2 years.
5	WECC2019021165	Yes		Yes	Yes								Yes	Category 1: 3 years; Category 2-
6	WECC2017017507	Yes		Yes	Yes					Yes				Category 2 – 12: 2 year
7	WECC2017017631	Yes		Yes	Yes					Yes				Category 2 – 12: 2 year
8	WECC2017017632	Yes		Yes	Yes					Yes				Category 2 – 12: 2 year
9	WECC2017017633	Yes		Yes	Yes				Yes	Yes				Category 2 – 12: 2 year
10	WECC2017017634			Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
11	WECC2017018364	Yes		Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
12	WECC2017017911	Yes		Yes	Yes			Yes		Yes				Category 2 – 12: 2 year
13	WECC2018018977	Yes		Yes	Yes			Yes		Yes	Yes			Category 2 – 12: 2 year
14	WECC2018019483	Yes		Yes	Yes			Yes		Yes				Category 2 – 12: 2 year
15	WECC2017018365			Yes	Yes					Yes	Yes			Category 2 – 12: 2 year
16	WECC2017017676	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2- 12: 2 years.

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
RFC2017018305	CIP-005-3a	R2	Medium	Severe	9/9/2014 (when the entity failed to implement all CIP-005-3a R2 protections on the	11/3/2017 (when the entity implemented the required controls	Self-Re				
Description of the Viola document, each violatio a "violation," regardless posture and whether it	tion (For purpose on at issue is desc s of its procedura was a possible, o	es of this cribed as l or	On August 30, 2017, the end 005-3a R2. This violation involves three	ntity submitted a Self-Report	t stating that, as a	5) Cyber Asset (BCA) without the use o	f certain				
confirmed violation.)			The entity's departments include <u>Remote Access characteris</u> to prevent a	The entity'sat the time employed reviews by multiple departments regarding firewall rules that allowed access in departments include When a firewall request was make the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access in the time employed reviews by multiple departments regarding firewall rules that allowed access the time employed reviews by multiple departments regarding firewall rules that allowed access the time employed reviews by multiple departments regarding firewall rules that allowed access the time employed reviews by multiple departments rules rules that allowed access the time employed reviews by multiple departments rules rules rules access the tintegret of time employed rules rules rul							
			In the first instance, entity without the required netw (procedure for securing dia	v staff identified that, beginni vork-level security controls re al-up access). A user would s	ing September 9, 2014, a equired by CIP-005-3a R2 Parts 2.1 (deny till have to authenticate to the applicati	y access by default), 2.2 (enable only p on prior to gaining access.	orts and				
			Additionally, regarding the second instance, the entity determined that the without the use of an Intermediate System, in violation of CIP-005-5 R2. The application log-on screen was reachable once the user logged in authentication, but it lacked an intermediate device. Thus, this second instance began July 1, 2016, when CIP version 5 went into effect.								
			Third, during an extent of condition review, the entity identified another instance where the BCAs responsible for host responsible for host . It was determined the access was granted on October 19, 2016. The entity completed remediation of this additional instance on No								
			The root cause of the viola missing a step to require v	ation is that the <u>entity lacked</u> rerification that	sufficient verification controls to ensur	e the configuration was correct for the	ŕ				
			The first violation (, and ended on May 9, 2017, when the entity implemented the required protections for the								
			The second violation implemented the required	controls on the device.) sta	rted on July 1, 2016, when CIP version	5 becam				
Rick Assassment			The third violation (relatin the required controls.	g to BCAs) start	ed on October 19, 2016, when the acces	ss was granted within an Intermediate	System,				
חוזע אספסטוופוונ			for CIP as a BES Cyber Syst authorized users the abilit	rem because its functionality y to view or change the cannot leverage the	is critical to other BES Cyber Systems. H	towever, y does not g	rant acce				
			Regarding the BCA in the t authorized administrators assessments, and scanned	hird instance, the BCAs do n after they have authenticate the assets quarterly. In add	ot perform any real-time BES functions. ed against the entity's access system. This is noted above, a user would still	Additionally, access to the assets was he entity was also monitoring for failed need to authenticate to the applicatio	only ava d authen on in orde				

ReliabilityFirst Corporation (ReliabilityFirst)

Settlement Agreement (Neither Admits nor Denies)

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
eport	2/9/2018	9/11/2018						
	<i>,</i> it	was in violation of CIP-						
n technical and procedural mechanisms for control of electronic provides a								
into the Electronic Security Perimeter (ESP). These hade, these departments reviewed the request for Interactive o ensure were properly configured on the								
was reachable directly from the entity's corporate user network d services required for operations and monitoring), and 2.3								
was reachable d nto the SSL VPN, v	irectly from the corpo which enforced encry	orate user network ption and multi-factor						
ting the lovember 3, 2017	e were direc	tly accessible via						
	and an insuffici	ent process which was						
mplement all CIP	-005-3a R2 protectior	ns on the						
me effective, and	ended on May 9, 201	7, when the entity						
a, and ended Nove	ember 3, 2017, when	the entity implemented						
Ilowing factors. 1 ess to any critical	The , real-time application	is in-scope n. It only permits						
us, the application vailable to interna ntication attempt ler to gain access;	has limited impact to l entity users, and acc s, performed annual o a logon screen would	o real-time operations. cess is granted only to cyber vulnerability d be presented to anyone						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho			
RFC2017018305	CIP-005-3a	R2	Medium	Severe	9/9/2014 (when the entity failed to implement all CIP-005-3a R2 protections on the	11/3/2017 (when the entity implemented the required controls	Self-Re			
			trying to access this applic the violation posed mode	cation. The entity also noted	that only authorized entity clients were k path available for assets potentially cr	allowed on the network, and that the	applicat			
Mitigation			For mitigation, generally, user or VPN networks) and also implemented a To mitigate this violation, 1) created new firewall r 2) held internal meeting 3) reviewed	as corrective measures, the e d implemented a procedural proce the entity: rules denying direct access fr s with Subject Matter Expert	entity removed the direct access by den . As pr control to update the dure that includes a reminder to add om all VPN networks and user networks s to determine approaches for preventin , tested as	ying traffic from VPN Networks and Us reventive measures, the entity implement to reject any firewall reques and to revie and to revie to reject any firewall request and to revie and to revie and to revie s needed, and remediated where neces	er Netw ented a sts from ew Remote a ssary;			
Other Factors			 4) deployed as noted in the root-cause explored as noted in the root-cause explored added which could accidentally grant direct access (additional); and 6) developed and published a procedure that instructs network analysts on configuring and provides a reminder to reverse and provides a reverse and provides a remander to reverse and provides a r							
			ReliabilityFirst considered were identified. The entit its violations, processes, s response in the future.	the entity's cooperation dur y voluntarily provided Reliab ystems, and organization, an	ing the Settlement Agreement process alityFirst with information regarding the ad this insight has allowed ReliabilityFirst	and awarded mitigating credit. The en violations in a manner that was thoro t to better analyze the violations. Relia	tity was ugh and abilityFir			
			Effective oversight of the Agreement. As a result, R	reliability of the BES depends eliabilityFirst seeks to encou	s on robust and timely self-reporting by rage this type of self-reporting by award	registered entities. The entity self-iden discussion of the self-iden discussion of th	ntified a			
			The entity has relevant co penalty. The prior noncor that the processes and sys	ompliance history. However npliances are distinguishable stems in place at the time of	, ReliabilityFirst determined that the en as they involved different circumstance the prior violations evolved such that th	tity's compliance history does not war as and root causes, in part because the a ne instant violations do not involve recu	rrant an amount urring cc			

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
eport	2/9/2018	9/11/2018						
tion servers were Ilicious acti <u>vity.</u>	not reachable via the	ese means. Regardless,						
rorks to the technical control to prevent any direct access into an ESP (from a User or VPN network to . The entity . The entity .								
Access to to use an Intermediate System;								
xplanation;	. This will help p	revent firewall rules from						
view firewall rule	s associated with							
proactive in working with ReliabilityFirst once the violations timely. The entity has been open with ReliabilityFirst regarding st awarded a mitigating credit to encourage this sort of								
nd reported some of the violations at issue in the Settlement								
elevated risk and of time that has p onduct.	d should not serve as bassed since mitigatio	a basis for an aggravated on supports the conclusion						

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				
RFC2016016353	CIP-007-3a	R2	Medium	Severe	4/24/2013 (9/30/2017 (Mitigation Plan completion)	Compliance Audit	9/30/2017	4/11/2018				
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			On October 11, 2016, Relia violation during a Complian ReliabilityFirst determined enabled, and therefore its of authorized were applicable justifications for the overly disabled. The root cause was the ent	iolation during a Compliance Audit conducted . .eliabilityFirst determined that the entity documented overly broad IP address port ranges. The entity did not make a sufficient determination to ensure that only those ports that were necessary were nabled, and therefore its documentation and baselines in its monitoring tool were overly broad in that they authorized an overly broad port range. In many instances, the unnecessary ports that were uthorized were applicable to all systems, which run the entity's most critical systems, including the energy management system. The entity could not produce ustifications for the overly broad port ranges. Additionally, in one instance, the entity did not identify an unauthorized port for a phone system that was deemed necessary because it could not be lisabled.									
Risk Assessment			The violations began on Ap This violation posed a mode for ports ranges is that an e authorizing overly broad po defense-in-depth measures port ranges, only necessary asset. Third, the entity em Remote Access sessions, ar reached from any local net access management and or regarding documenting por and move laterally into one	The violations began on April 24, 2013,									
Mitigation Other Factors			 To mitigate this violation, the entity: 1) developed evidence standards that require vendor, design, or architectural justification for necessary ports, as well as evidence storage and metadata for cataloging necessary ports; 2) demonstrated effectiveness of new evidence requirements and validated necessary ports and services for the CIP cyber assets chosen in the addited action of the evidence requirements into the entity's ports and services and procedures; 3) integrated the evidence requirements into the entity's ports and services policies and procedures; 4) iterated through the remaining CIP-scoped cyber assets to ensure compliance with new evidence requirements defined in milestone 2, updated the catalog of necessary ports as necessary, and verified open ports on the assets with approved list; and 5) completed iteration of the remaining CIP-scoped cyber assets 5) completed iteration of the remaining CIP-scoped cyber assets 6) the catalog of necessary ports as necessary, and verified open ports on the assets with approved list. 										
			ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. The entity was proactive in working with ReliabilityFirst once the violations were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was thorough and timely. The entity has been open with ReliabilityFirst regarding ts violations, processes, systems, and organization, and this insight has allowed ReliabilityFirst to better analyze the violations. ReliabilityFirst awarded a mitigating credit to encourage this sort of response in the future.										

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
RFC2016016353	CIP-007-3a	R2	Medium	Severe	4/24/2013 (9/30/2017 (Mitigation Plan completion)	Compliance Audit	9/30/2017	4/11/2018
			Effective oversight of the r Agreement. As a result, Re The entity has relevant cor penalty. The prior noncom conclusion that the proces	eliability of the BES depends eliabilityFirst seeks to encours npliance history. However, F npliances are distinguishable ses and systems in place at th	on robust and timely self-reporting by r age this type of self-reporting by award ReliabilityFirst determined that the entit as they involved different circumstance ne time of the prior violations evolved s	registered entities. The entity self-ider ing some mitigating credit. cy's compliance history does not warra is and root causes, in part because the uch that the instant violations do not i	ntified and reported som nt an elevated risk and s amount of time that has nvolve recurring conduc	e of the violations at hould not serve as a s passed since mitigat t.	issue in the Settlement basis for an aggravated ion supports the

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
RFC2017018475	CIP-010-2	R1	Medium	Severe	4/26/2017 (when the entity user installed the unauthorized application)	7/18/2017 (when the application was ultimately removed from the server)	Self-Re				
Description of the Violat	tion (For purpose	es of this	On October 5, 2017, the e	ntity submitted a Self-Report	stating that, as						
document, each violatio	n at issue is desc	ribed as									
a "violation," regardless	of its procedura	l	On April 26, 2017, an entit	e analyst installed an unautr	iorized application in his personal hon	ne directory on an Electronic Access Co	ntrol or N				
confirmed violation.)	was a possible, t	,	application was used by the application was not detect changes.	al's home directory did <u>not r</u> ted by the entity's tool,	equire escalated privileges, so the ana because the software was installe	alyst did not believe he needed to file a ed in the analyst's home directory, whic	change n ch is not s				
			However, on April 27, 201 investigated the issue, shu	7, the entity's sectors port s It down the unauthorized po	scans detected the presence of an una rt, and subsequently notified the anal	authorized port which was which was yst that the software was not authorized	is attribut ed.				
			On May 3, 2017, the analy expressed security concern application to the entity's port scans detect	est initiated the entity's softwars ns with the software and offer security review team, which ed the unauthorized port, ar	vare approval process, but the request ered alternative applications for the a was considered, and ultimately denie nd, in each instance, the entity's IT tea	t to utilize the application was denied o nalyst to utilize. As part of the review p d on July 12, 2017. In the meantime, th ms shut down the unauthorized port.	n May 25 process, th he analyst				
			On July 11, 2017, the entity performed a review of recent changes to the authorized port "whitelist" and noticed the unauthorized port on a . Upon discovery, the entity investigated the issue and discovered that was still installed on a CIP Intermediate System								
			The application remained in use and actively opened ports from April 26, 2017 to July 18, 2017, when the application was ultimately remove on the server for 83 days, therefore exceeding the required time (30 days) the entity had after installation to update the baseline. Additiona activities before installing the application.								
			The root causes were lack of understanding on when change management requests were required, insufficient controls to detect the unaut analyst removed the application. This violation involves the management practices of workforce management, in that additional training co configuration management, in that the entity's controls were insufficient to detect and manage changes to its assets.								
			This noncompliance starte	d on April 26, 2017, when th	e entity user installed the unauthorize	ed application, and ended July 18, 2017	', when th				
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the fol could have introduced vulnerabilities into the system or could have adversely affected the functionality of the EACMS. This risk was somewh accepted connections from clients after the client logged into a VPN with two-factor authentication and authenticated to the Intermediate S likelihood that someone could successfully access the application and potentially compromise the bulk power system. However, the risk is s prior to installation. Additionally, although the entity quickly identified the unauthorized application, the entity failed to ensure that the app								
Mitigation			To mitigate this violation,	the entity:							
			 removed the unauthor counseled the analyst scanned for changes to implemented a tool to inspected the results of modifications to the b 	rized application from the sy and the department staff on o the home directory of the o scan home directories on Cl of the initial home directory s aselines as needed.	stem; the importance of following the entit machine at issue. The entity refined of P-scoped systems to look for sc scans on assets for additional ex	ty's configuration and change managen letection rules to ensure scripts and sof ripts and locally installed software; and ceptions, determined if modifications t	nent proce ftware in t o the app				
Other Factors			ReliabilityFirst reviewed th	ne entity's internal compliand	ce program (ICP) and considered it to	be a neutral factor in the penalty deter	mination.				
			1								

ReliabilityFirst Corporation (ReliabilityFirst)

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation							
eport	6/21/2018	11/29/2018							
, it was in vio	, it was in violation of CIP-010-2 R1.								
Ionitoring System (EACMS) Intermediate System. The . The work to install the									
nanagement request (or test the application). The unauthorized subject to routine scans used to detect software									
ted to the	ed to the entity's IT team								
5, 2017. At that time, the entity's security review teams he analyst provided further business justification to utilize the t continued to utilize . The entity's									
CIP Intermediate	e System, attributable	to the							
ed from the serve ally, the user did r	r. The application wa not perform the requi	s installed and was in-use red change management							
horized applicatic uld have helped p	on, and the entity's fa prevent the violation,	ilure to verify that the and asset and							
ne application wa	s ultimately removed	from the server.							
lowing factors. The potential risk was that the application nat mitigated by the following factors. The application only system through the sector . Thus, there was low till moderate because the entity failed to test the application plication was removed, and the unauthorized application ne system.									
esses and clarified aspects of baselines; the home user directories are detected;									
proved baselines a	are needed, and train	ed individuals on the							

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
DEC2017010475		D 1	N de alicense	Courses	4/26/2017 (when the entity user	7/18/2017 (when the application	Colf Domont	C /21 /2010	11/20/2010
RFC2017018475	CIP-010-2	KI	Iviedium	Severe	application)	server)	Self-Report	6/21/2018	11/29/2018
			 KenabilityFirst considered were identified. The ent its violations, processes, response in the future. Effective oversight of the Agreement. As a result, The entity has relevant c required). However, RF o prior noncompliances, qu 	ity voluntarily provided Reliab systems, and organization and reliability of the BES depends ReliabilityFirst seeks to encour ompliance history. Some of th did not aggravate the penalty uickly identified and corrected	ilityFirst with information regarding the d this insight has allowed ReliabilityFirst on robust and timely self-reporting by rage this type of self-reporting by award ne prior noncompliances resulted from based on repeat behavior because the noncompliances.	registered entitigating credit. The entity to better analyze the violations. Relial registered entities. The entity self-ider ling some mitigating credit. arguably similar contributing causes (i.e prior noncompliances were all minimal	and timely. The entipolity First awarded a mition officed and reported som e. lack of understanding risk and involved high-fr	thig with Kellability ity has been open wit igating credit to enco ne of the violations at on when change man requency conduct for	issue in the Settlement agement requests were which the entity, in the

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
RFC2018019404	CIP-010-2	R2	Medium	Severe	5/24/2017	2/20/2018 (when the entity remediated the baseline configuration issue)	Self-R				
Description of the Violat	tion (For purpose	s of this	On March 13, 2018 and Ap	ril 17, 2018, the entity subm	itted Self-Reports stating that, as	a					
document, each violatio a "violation," regardless posture and whether it v confirmed violation.)	n at issue is desc of its procedura was a possible, c	ribed as l or	This violation includes two 10-2 R2.1. On May 24, 201 baseline monitoring tool internal controls testing.	separate instances. In the f 7, four firewalls which are cl and were	irst incident, the entity did not mo assified as Electronic Access Contr e not monitored for baseline chan	nitor a baseline configuration for four (ol or Monitoring Systems (EACMS) wer ges until November 30, 2017, when an	CIP-scoped as e placed into entity analys				
			In the second incident, the July 5, 2017, the entity per the upgrade failed. Howeve acceptable and not investig assets were affected and d	entity did not monitor two I formed an upgrade on two F er, because the entity's mon gated further. On January 9, iscovered the second advers	Protected Cyber Assets (PCAs) at le PCAs which caused some of the ba itoring tool was able to reconcile to 2018, an analyst discovered the is sely affected asset.	east once every 35 days for changes to seline elements to return an error in th the error with a change ticket for the up sue on one asset and immediately rem	the baseline e entity's mo ograde, the c ediated it. Or				
			There were different root causes for the two incidents in this violation. In the first incident, the process for configuration management was a responsibility it was to notify the entity's monitoring tool to monitor the baseline element; and since the process was unclear, it was not foll of configuration monitoring. In the second incident, the file-retrieving software used by was older than the version on the entity's cretrieving software had communication issues which resulted in an error communication. However, the error was not caught because the in change ticketing system was limited. Ilimitations in integration caused to erroneously reconcile a baseline change from July 5, 2017, with a change ticket for the affected an error, rather than the change recorded in the change ticket.								
			This violation involves the management practice of verification because there was an error in the entity's verification process in that, during with the change ticket.								
			This noncompliance started on May 24, 2017, which is the date the firewalls were placed into service in the first instance and ended on February configuration issue.								
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system based on the fol for an unauthorized user to change the baseline configuration without the entity's knowledge. The risk is partially reduced because in the se affected by the violation. Further reducing the risk, all other CIP controls were in place for the affected assets in the second incident. includir a threat caused by the failure to monitor the firewalls. Minimizing the risk in the first incident, in order to reach the firewalls from an admini use of an Intermediate Device; further all Bulk Electric System (BES) Cyber Asset and PCAs behind the firewalls were also afforded all protect incident had a duration of more than 7 months before it was discovered by the entity's internal controls.								
Mitigation			To mitigate this violation, t	he entity:							
			 created an "Awareness Only" ticket in the entity change management system to enable daily scans on the affected a assets daily; performed a reconciliation to ensure no other assets were affected; reviewed the scans for the affected assets per the entity's scans. No actions needed, identified/documented the root cause of the configuration difference for the affected assets. The entity created a ticket with request to performed a reconciliation to discover any other assets affected with older version of a file-retrieving software; held a meeting to determine process improvement steps; updated the two affected assets with current version of a file-retrieving software. The entity ran scan successfully to ensure all 								

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
eport	7/31/2018	11/19/2018						
	, it was in violation	on of CIP-010-2 R2.						
ssets at least once every 35 calendar days as required by CIP- o service; however, the firewalls were not added to the entity's st detected the violation while seeking evidence for the entity's								
configuration as required by CIP-010-2 R2. As background, on onitoring tool and the second s								
not properly documented which made it unclear whose owed effectively, resulting in the four EACMS being left outside other similar devices. Therefore, the older-version of the file- tegration between the system and the These								
asset for the sam	e day; however, the a	actual change was due to						
the verification p ruary 20, 2018, wi	process, the error was hen the entity remedi	incorrectly reconciled						
llowing factors. T	he risk posed by this	violation is the potential						
cond incident jus ng logs and anti-v istration perspect tions as defined b	t 2 of the entity's irus protection which ive required two-fact y the NERC CIP Stand	PCAs were would alert the entity to or authentication and the ards. However, the first						
ssets. The entity configured to scan the affected								
l, no changes dete o resolve issue;	, no changes detected; resolve issue;							
l configuration ba	seline elements are b	eing monitored;						

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
RFC2018019404	CIP-010-2	R2	Medium	Severe	5/24/2017	2/20/2018 (when the entity remediated the baseline configuration issue)	Self-Report	7/31/2018	11/19/2018
 8) updated the entity's Procedure to add how to The entity communicated this change to the team; 9) collected and created an inventory of all error types for content scans within the entity 10) configured test environment of to identify unexpected content so that a scanning error veconfiguration solution to determine review frequency and overall process with the entity; 11) validated that implementation was successful and provided expected data that will assist in error future content exceptions originating from unknown errors; and 12) trained staff on new second process and how to adjust for future inclusion. 						The entity created an inventory based or t a scanning error will pick up specific changes like t will assist in error identification and baseline rec inclusions.	en to configure n previously identified en e a new version of a file-r onciliation. The entity de	to monitor ror types; retrieving software. T ocumented process fo	CIP baseline elements. The entity integrated a or implementation in
Other Factors ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty de ReliabilityFirst reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty de ReliabilityFirst considered the entity's cooperation during the Settlement Agreement process and awarded mitigating credit. Th were identified. The entity voluntarily provided ReliabilityFirst with information regarding the violations in a manner that was th its violations, processes, systems, and organization and this insight has allowed ReliabilityFirst to better analyze the violations. F response in the future. Effective oversight of the reliability of the BES depends on robust and timely self-reporting by registered entities. The entity self Agreement. As a result, ReliabilityFirst seeks to encourage this type of self-reporting by awarding some mitigating credit. The entity has relevant compliance history. However, ReliabilityFirst determined that the entity's compliance history does not v penalty. The prior noncompliances are distinguishable as they involved different circumstances and root causes, in part because conductions that the nencess and outcomes and not causes and outcomes and root causes.					ered it to be a neutral factor in the penalty detern ent process and awarded mitigating credit. The en egarding the violations in a manner that was thoro liabilityFirst to better analyze the violations. Relia eporting by registered entities. The entity self-ide ng by awarding some mitigating credit. that the entity's compliance history does not warr circumstances and root causes, in part because the ns evolved such that the instant violations do not	nination. Itity was proactive in worugh and timely. The ent bilityFirst awarded a mit ntified and reported som ant an elevated risk and amount of time that ha involve recurring conduc	rking with ReliabilityF ity has been open wit igating credit to enco ne of the violations at should not serve as a s passed since mitigar ct.	irst once the violations h ReliabilityFirst regarding urage this sort of issue in the Settlement basis for an aggravated tion supports the	

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
WECC2019021165	CIP-010-2	R1; P1.4.1; P1.4.2; P1.4.3; P1.5.1; P1.5.2	Medium	Severe	2/14/2019 (when the entity changed the configuration by removing the software)	2/26/2019 (when the entity assessed the security controls according to CIP-010)	Self-Report	2/26/2019	6/11/2019
Description of the Viol document, each violat "violation," regardless whether it was a possi Risk Assessment	ation (For purpos ion at issue is des of its procedural ble or confirmed	es of this cribed as a posture and violation.)	On March 5, 2019, the en of a daily delta report for Cyber Systems (HIBCS) loc environment, had interface sending false errors to the error reporting. The could be impacted by the CIP-010-2 R1 Part 1.4 sub such testing as required by have been adversely affect After reviewing all relevant personnel deciding to not performing the work, the WECC determined this iss existing baseline configuration controls were not adverse results prior to implement BCA to another, which co However, in this instance good detective controls in isolated incident and not	tity submitted a Self-Repor baseline configuration char cated at the primary and bac ces used to send data from e software vendor through a BCAs were then turned on, a change or verifying that ar -parts 1.4.1, 1.4.2, and 1.4.3 y CIP-010-2 R1 Part 1.5 sub- cted, the verification results the information, WECC Enfor- follow the entity's change y determined the removal of ue posed a moderate risk a ation related to BCAs, t ely affected; and document ting the change as required uld potentially affect the rel the interfaces on the BCA we in the form of a daily delta re- condoned by the entity's m	t stating, as a as nges , the entity identified ckup Controls Centers that had softwo one server to the other, turned off be a different connection than the interf at which time the software removal of ny identified cyber security controls of 3. Additionally, the entity did not tes -parts 1.5.1 and 1.5.2 This issue ender were documented, and the baseline control and configuration management of the software posed no threat to the and did not pose a serious or substant the entity failed to determine required the results of the verification as required the results of the specification as required the results of the verification as required the results of the BPS.	, it was in potential noncompliance Bulk Electric are removed on February 14, 2019. The ecause the BCAs were scheduled to be face, resulting in the software vendor occurred without the entity first deter were not adversely affected, once the t the changes in a production or test ed on February 26, 2019, when the se change was documented, for a viola CIP-010-2 R1 Parts 1.4 and Part 1.5 and ent processes. Specifically, based on the BPS and therefore, completed the was tial risk to the reliability of the bulk part d cyber security controls in CIP-005 and ined by CIP-010-2 R1 Part 1.4, as well e could have caused the BCA interfact and the servers; therefor ges which is how this issue was disco poor of a future issue. No harm is knowed the test of a future issue. No harm is knowed the test of a future issue. No harm is knowed the test of the test of the servers is the test of the test of the servers is the test of the test of the test of the test of tes	e with CIP-010-2 R1. Specific System (BES) Cyber A The BCAs, although the decommissioned. The r calling the entity and in rmining the required cylone change had taken plate the change	ecifically, on February ssets (BCAs) associated connected to the netw e software, which was nitiating the software per security controls in ce; nor documenting a mplementing the chan 05 and CIP-007 were d c. root cause of the issue ledge of the senior per documented change m his instance, for a char e impacted by the chan oduction or test enviro e and affect traffic that was lessened. The enti- nfirmed the root cause	16, 2019, during a review d with its High Impact BES rork and in the production part of the interface, was removal to solve the false of CIP-005 and CIP-007 that any results as required by use and did not document etermined, verified to not e was attributed to senior rsonnel and a contractor nanagement processes. Inge that deviated from an use; verify those identified nment and document the t was being sent from one ty had implemented e of this violation was an
Mitigation			To remediate and mitigat 1) verified the secur 2) updated its baseli 3) created awarenes 4) confirmed that th	e this issue, the entity has: ity controls of the baseline ine configuration for a chan as of the importance of follo ie individual responsible for	configuration change and documente ge that deviated from an existing bas wing the change management procee causing the violation is no longer wit	ed the verification; seline configuration; dures by sending a security awarenes th the entity.	ss email to personnel wit	h authority to implem	ent baseline changes; and
Other Factors			WECC reviewed the entity includes a process for self WECC considered the ent	y's internal compliance prog -auditing and monitoring fo ity's history of noncomplian	gram (ICP) and considered it to be a n or noncompliance which is how this v nce with CIP-010-2 R1 given NERC Vio	nitigating factor. The entity exercised iolation was discovered. lation ID	I due diligence to detect ermined it should not se	this violation. Addition	onally, the entity's ICP avating the penalty
			WECC considered the ent	ity personnel's choice not to	o follow the Standard and Requireme	ent to be an aggravating factor in trea	ating this violation in a S	ettlement Agreement	instead of as an FFT.

NOC-2658

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation		
WECC2017017507	CIP-005-5	R1: P1.1	Medium	Severe	07/01/2016	07/25/2017	Self-Report	12/04/2018	02/22/2019		
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)			it was in potential noncompliance with CIP-005-5 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one within the Electronic Security Perimeter (ESP), and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA and submitted four additional Self-Reports. After reviewing all relevant information, WECC determined the entity failed to place the BCA connected to a network via a routable protocol, within a defined ESP as required by CIP-005-5 R1 Part 1.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on July 25, 2017, when the BCA was added to the ESP, for a total of 390 days of noncompliance.								
Risk Assessment			The root cause of the BCA WECC determined these	violations was attributed t violations (WECC201701756	o a lack of knowledge of the ca 07, WECC2017017631, WECC2	pabilities and functions of the BCA. 017017632, WECC2017017633 and V	VECC2017017634) individu	ually and collectively pos	sed a minimal risk and did		
			and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and PACS correscribed herein and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a second which could affect correct at the entity; thereby potentially affecting the reliability of the BPS. Failing to create a baseline for configuration results in the entity not being able to compare the current configuration to that which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.								
			However, as compensation the entity's network, prev located within a PSP. The system would automatica and could have utilized hi implemented periodic int	n, the entity had implemen renting the BCA from being BCA was used as a Ily switch to one of the back s capability to quickly switch ernal audits which is how th	ted managed policy rules for n accessed from other network s , kup sources within 30 seconds h the to o ne instances with the EACMS a	nonitoring the BCA, and it was in a net segments unless a specific rule was cro but there were two backup sources If ne of the backup devices, in the event nd PACS were discovered.	work segment that limited eated to allow that commu . If the primar , the s they needed to manually	d permissions to commun inication path. To contro y (th System Operator would h bypass the BCA. Addition	icate with other parts of physical access, it was e BCA) were to fail, the ave received an alarm nally, the entity		
Mitigation			To mitigate this violation, 1) placed the BCA in 2) trained techniciar	the entity has: side the ESP; and is to increase their knowled	lge of legacy devices and the fu	inctionality of those devices.					
Other Factors			These violations (WECC20 WECC2017018365) posed Expedited Settlement Agr	17017507, WECC20170176 a minimal risk to the reliak eement with a \$0 penalty.	31, WECC2017017632, WECC2 pility of the BPS. However, due	017017633, WECC2017017634, WECC to the number of violations and Cybe	2017017911, WECC20180 r Assets in scope, WECC es	18977, WECC2018019483 scalated the disposition t	, and reatment to an		
			WECC considered the ent	ity's compliance history and	d determined there were no re	evant instances of noncompliance.					

NOC-2658

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017631	CIP-007-6	R1: P1.1	Medium	High	07/01/2016	05/17/2017	Self-Report	09/07/2017	10/08/2019
Description of the Violat document, each violation "violation," regardless of and whether it was a pos violation.)	iption of the Violation (For purposes of this ment, each violation at issue is described as a ation," regardless of its procedural posture whether it was a possible or confirmed tion.) On May 22, 2017, the entity submitted a Self-Report stating, as a a Self-Report stating,								, it of one within the 3CS). The BCA was located the same BCA. d by the entity as required ne BCA's open logical ports
Risk Assessment			WECC determined these risk and did not pose a se R2, and R5, and CIP-010-2 Failing to locate this BCA fail or manipulate a the entity not being able allow an attacker entry to effects on the Cyber Asse However, as compensation entity's network, prevent within a PSP. The BCA wa automatically switch to o utilized his capability to o audits which is how the in	violations (WECC201701750 rious and substantial risk to 2 R1 to one BCA as described within an ESP and provide it which a to compare the current com o the device. Failing to obtain ts and the BES. Failing to tim on, the entity had implement ing the BCA from being acce as used as a ne of the backup sources with uickly switch the stances with the EACMS an . No ha	07, WECC2017017631, WECC20170 o the reliability of the Bulk Power S d herein and provide the protective t the protective measures of the S could affect of the second at the em- figuration to that which was recor- in authorization for changes to ba- nely update baseline configuration ated managed policy rules for mon essed from other network segmen , but there we ithin 30 seconds. If one of the backup de and PACS were discovered.	D17632, WECC2017017633 and WECC201701 System (BPS). In these instances, the entity for e measures of CIP-010-2 R1 to EACMS and tandards and Requirements could increase t tity; thereby potentially affecting the reliabil mmended and approved. Open ports and ser seline configurations could result in misconf his could lead to incorrect assumptions which itoring the BCA and it was in a network segn ts unless a specific rule was created to allow were two backup sources for the second second second second second second second to allow were two backup sources for the second sec	17634) individually and of ailed to provide the pro- and PACS as describ- the risk of it being remot ity of the BPS. Failing to rvices, for instance, could igurations and potential of could result in failure of nent that limited permise that communication pare e primary e System Operator woul by by pass the BCA. Addition	ollectively posed a m tective measures of C bed herein. ely accessed by an att create a baseline for d be open without kn ly lead to diminished r manipulation of Cyb sions to communicate th. To control physica (the BCA) were d have received an al phally, the entity impl	nimal IP-005-5 R1, CIP-007-6 R1, acker with the intent to configuration results in owledge of the entity and abilities or unanticipated er Assets. with other parts of the al access, it was located e to fail, the system would arm and could have emented periodic internal
Mitigation			To mitigate this violation, 1) documented all e 2) trained technicia	the entity has: nabled logical network acce ns to increase their knowled	essible ports; and Ige of legacy devices and the func	ionality of those devices.			
Other Factors			These violations (WECC20 posed a minimal risk to the Agreement with a \$0 per WECC considered the ent	017017507, WECC20170176 ne reliability of the BPS. How alty. ity's compliance history and	31, WECC2017017632, WECC2017 vever, due to the number of violat d determined there were no releva	017633, WECC2017017634, WECC20170179 ions and Cyber Assets in scope, WECC escala ant instances of noncompliance.	11, WECC2018018977, Vated the disposition trea	VECC2018019483, an Itment to an Expedite	d WECC2017018365) d Settlement

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017017632	CIP-007-6	R2: P2.1	Medium	Moderate	07/01/2016	05/09/2017	Self-Report	08/24/2018	10/23/2019
Description of the Viola document, each violatio "violation," regardless of and whether it was a po violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a was in potential noncompliance with CIP-007-6 R2. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of or the Electronic Security Perimeter (ESP), used as the security and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The entity discovered it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the security firmware patches are as required by CIP-007-6 R2 Part 2.1. This violation began on July 1, 2016, when the Standards and Requirements became mandatory and enforceable, and ended on May 9, 2017, added to the patch source tracking spreadsheet, for a total of 313 days of noncompliance.								, it nt of one within IBCS). The BCA was located o the same BCA. ches applicable to the BCA, , 2017, when the BCA was
Risk Assessment			WECC determined these violation was attributed to a lack of knowledge of the capabilities and infittions of the BCA. WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633 and WECC2017017634) individually and collectively posed a minin risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-01-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to Methods and Methods an						inimal IP-005-5 R1, CIP-007-6 R1, ttacker with the intent to r configuration results in nowledge of the entity shed abilities or ipulation of Cyber Assets. te with other parts of the cal access, it was located re to fail, the system red an alarm and could ty implemented periodic
Mitigation			. No harm is known to have occurred. To mitigate this violation, the entity has: 1) added the BCA to the patch source tracking spreadsheet; 2) trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and 3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected to the operations network or deployed into an ESP to inclading Cyber Assets to the patch tracking spreadsheet and documenting baseline configurations.						yed into an ESP to include
Other Factors			ECC determined that the indicative of broader co	e entity's compliance history mpliance issues.	should not serve as a basis for aggrava	ting the penalty because the previous	relevant history was an i	ssue in 2014 that pos	ed minimal risk and not

NOC-2658

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation			
WECC2017017633	CIP-007-6	R5: P5.1- P5.7	Medium	Severe	07/01/2016	02/15/2019	Self-Report	02/15/2019	TBD			
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)		On May 22, 2017, the entity submitted a Self-Report stating, as a self-was in potential noncompliance with CIP-007-6 R5. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one within the Electronic Security Perimeter (ESP), used as the self-meter (ESP), used as the self-meter (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA. After reviewing all relevant information, WECC determined the entity failed to have method(s) to enforce authentication of interactive user access, identify and inventory all known enabled default or										
other generic account types, identify individuals who have authorized access to shared accounts, change known default passwords, enforce the required password length and complex changes at least once every 15 calendar months; and limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentic technically feasible on the BCA, as required by CIP-007-6 R5 Parts 5.1 through 5.7. This violation began on July 1, 2016, when the Standards and Requirements became mandatory ended on February 15, 2019, when the protective measures as required by CIP-007-6 R5 Parts 5.1 through 5.6 were implemented and for Part 5.7 when the entity submitted Exception, for a total of 960 days of noncompliance.								nplexity, enforce password entication attempts where atory and enforceable, and eted a Technical Feasibility				
Risk Assessment			WECC determined these violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, and WECC2017017634) individually and collectively posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In these instances, the entity failed to provide the protective measures of CIP-005-5 R1, CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and CIP-010-2 R1 to one BCA as described herein and provide the protective measures of CIP-010-2 R1 to EACMS and the comparison of the set of the protective measures of CIP-010-2 R1 to EACMS and the comparison of the comp									
			Failing to locate this BCA within an ESP and provide it the protective measures of the Standards and Requirements could increase the risk of it being remotely accessed by an attacker with the intent to fail or manipulate a primary which could affect which could affect which was recommended and approved. Open ports and services, for instance, could be open without knowledge of the entity and allow an attacker entry to the device. Failing to obtain authorization for changes to baseline configurations could result in misconfigurations and potentially lead to diminished abilities or unanticipated effects on the Cyber Assets and the BES. Failing to timely update baseline configurations could lead to incorrect assumptions which could result in failure or manipulation of Cyber Assets.									
			However, as compensate entity's network, preven within a PSP. The BCA we would automatically sw have utilized his capabili internal audits which is	tion, the entity had implementing the BCA from being acc vas used as a itch to one of the backup so ity to quickly switch the how the instances with the B	nted managed policy rules for monitori cessed from other network segments ur , but there were urces within 30 seconds. If to one of the backup of ACMS and PACS were discovered. . No harm is known to have occurre	ng the BCA and it was in a network seg nless a specific rule was created to allow two backup sources for . If the levices, in the event they needed to ma ed.	ment that limited permi w that communication p ne primary , the System Operat anually bypass the BCA.	ssions to communica ath. To control physic (the BCA) we or would have receiv Additionally, the entir	te with other parts of the cal access, it was located re to fail, the system ed an alarm and could ty implemented periodic			
Mitigation			 enforced authentication of interactive user access by changing the default passwords; identified and inventoried all default accounts; added new passwords to password safe and only allowed access to technicians with authorization to shared accounts in the password safe; changed the default passwords for all accounts; procedurally enforced password requirements; tracked password changes in account database to be changed at least every 15 calendar months; submitted to WECC a Technical Feasibility Exception for the Cyber Assets in scope not capable of limiting the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts; trained technicians to increase their knowledge of legacy devices and the functionality of those devices; and 									
			9) implemented a bi-weekly or monthly CIP collaboration meeting between technical personnel, the CIP subject matter experts, the management to discuss such details as review of default accounts, passwords, account access logging, and asset name/role tags during the annual cyber vulnerability assessments.									

	NOC-2658
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WEC posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the Agreement with a \$0 penalty.
	WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant posed minimal risk and are not indicative of a broader issue.

ECC2018018977, WECC2018019483, and WECC2017018365) ne disposition treatment to an Expedited Settlement

ant history consisted of an issue in 2011 and one in 2014 that

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation		
WECC2017017634	CIP-010-2	R1: P1.1; P1.2; P1.3	Medium	Moderate	07/01/2016	05/18/2017	Self-Report	11/16/2018	08/13/2019		
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)		es of this cribed as a posture and violation.)	On May 22, 2017, the entity submitted a Self-Report stating, as a self-was in potential noncompliance with CIP-010-2 R1. Specifically, during an internal audit conducted on April 26, 2017, the entity discovered it had not completed the placement of one within the Electronic Security Perimeter (ESP), used as the self-was in and classified as a BES Cyber Asset (BCA) associated with a Medium Impact BES Cyber System (MIBCS). The BCA was located within a Physical Security Perimeter (PSP). On May 9, 2017, the entity determined it had not provided the protective measures of CIP-007-6 R1, R2, and R5, and CIP-010-2 R1 to the same BCA.								
			The Self-Report submit 1.1.4; for EACMS a same PACS, made Part 1.3.	ted for CIP-010-2 R1 also ind and PACS, the entity face changes that deviated from	cluded noncompliance related to t ailed to authorize and document m the existing baseline configurati	hree EACMS that did not have logical port in changes that deviated from the existing bas on without updating the baseline configurat	nformation in the baselir eline configuration as re tion within 30 calendar o	ne configuration as re equired by Part 1.2; a days from completing	quired by Part 1.1 sub-part nd for EACMS and the the change as required by		
			After reviewing all relevent of the second s	vant information, WECC det ne configuration for the ing baseline configuration f leting a change that deviat mandatory and enforceab P-010-2 R1 instances related	Exermined the entity failed to devel ACMS that included any logical n for EACMS and EACMS as ted from the existing baseline co le, and ended on May 18, 2017, d to the EACMS and PACS ended on	op baseline configurations for the BCA firmv etwork accessible ports as required by CIP-0 required by Part 1.2; and update the baselin nfiguration as required by CIP-010-2 R1 Pa when a port scan was completed, and the n June 7, 2017, when baseline configurations	ware and a port as requi D10-2 R1 Part 1.4 sub-part the configuration for rt 1.3. This violation back BCAs baseline configu- s were authorized and up	red by CIP-010-2 R1 P art 1.1.4; authorize an EACMS and EACMS and P egan on July 1, 2016 ration was updated, odated, for a total of 3	Part 1.1 sub-parts 1.1.1 and nd document changes that ACS as necessary within 30 , when the Standards and for a total of 322 days of 42 days of noncompliance.		
			The root cause of the E to less than adequate t	CA violations was attribute raining and miscommunicat	d to a lack of knowledge of the ca ions. Specifically, steps were over	pabilities and functions of the BCA. The roo looked or not performed correctly because t	t cause of the violations hey were being perform	s related to the EACM ned infrequently.	S and PACS was attributed		
Risk Assessment			WECC determined the pose a serious and sub and CIP-010-2 R1 to on	se violations (WECC201701) stantial risk to the reliability e BCA as described herein a	7507, WECC2017017631, WECC20 y of the Bulk Power System (BPS). nd provide the protective measur	17017632, WECC2017017633, and WECC201 In these instances, the entity failed to prov es of CIP-010-2 R1 to two EACMS and three	17017634) individually a vide the protective meas PACS as described herei	nd collectively posed sures of CIP-005-5 R1 n.	a minimal risk and did not , CIP-007-6 R1, R2, and R5,		
			Failing to locate this BC fail or manipulate a the entity not being ab and allow an attacker e unanticipated effects o Assets.	A within an ESP and provide which le to compare the current co ntry to the device. Failing t n the Cyber Assets and the	e it the protective measures of the ch could affect at the e onfiguration to that which was rec o obtain authorization for changes BES. Failing to timely update base	e Standards and Requirements could increase entity; thereby potentially affecting the relial commended and approved. Open ports and s s to baseline configurations could result in m ine configurations could lead to incorrect as	e the risk of it being rem bility of the BPS. Failing services, for instance, co hisconfigurations and po ssumptions which could	otely accessed by an to create a baseline fo uld be open without tentially lead to dimin result in failure or ma	attacker with the intent to or configuration results in knowledge of the entity hished abilities or nipulation of Cyber		
			However, as compensa entity's network, preve within a PSP. The BCA would automatically sw have utilized his capabi internal audits which is	tion, the entity had implem nting the BCA from being ac was used as a vitch to one of the backup so lity to quickly switch the how the instances with the	ented managed policy rules for ma ccessed from other network segm , but there ources within 30 seconds. If to one of the ba EACMS and PACS were discovere No harm is known to h	onitoring the BCA and it was in a network se ents unless a specific rule was created to allo e were two backup sources . If ackup devices, in the event they needed to m d. ave occurred.	gment that limited perm ow that communication the primary , the System Opera nanually bypass the BCA	nissions to communic path. To control phys (the BCA) w ator would have recei . Additionally, the ent	ate with other parts of the ical access, it was located ere to fail, the system ved an alarm and could city implemented periodic		
Mitigation			To mitigate this violation 1) updated and and 2) trained technic	on, the entity has: uthorized baseline configura ians to increase their knowl	ations on the Cyber Assets in scope edge of legacy devices and the fur	e of these violations; nctionality of those devices;					

Western Electricity Coordinating Council (WECC)

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

	NOC-2658					
	 3) updated its process to require all new Cyber Assets to go through a documented commissioning process before being connected documenting baseline configurations; and 4) updated the change management software to require: 					
	 a. a documented baseline configuration be completed as part of the commissioning process before deploying into an ESP; b. employees to update the baseline configuration on Cyber Assets before they can close the request for change. 					
Other Factors	These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, W posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated t Agreement with a \$0 penalty.					
	WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.					

ed to the operations network or deployed into an ESP to include

and

VECC2018018977, WECC2018019483, and WECC2017018365) the disposition treatment to an Expedited Settlement

Ν	O	C-	.7	6	52	8
	\sim	<u> </u>	~	v	-	•

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho			
WECC2017018364	CIP-006-6	R1: P1.5	Medium	Severe	07/01/2016		Com			
Description of the Violat document, each violatio a "violation," regardless posture and whether it v confirmed violation.) Risk Assessment	ion (For purpose n at issue is desc of its procedural vas a possible or	s of this ribed as	During a Compliance Audit conducted , had a potential noncompliance with CIP-006-6 R1 Parts 1.4 and 1.5. Specifically, for the demonstrate that it was monitoring for unauthorized access through a physical access point into each PSP as required by CIP-006-6 R1 Part access through a physical access point into each PSP were issued to the personnel identified in the BES Cyber Security Incident response plan 1.5. The root cause of the violation was attributed to a misinterpretation of the Requirement Parts. Specifically, the entity believed if the PSPs w was needed, as such, the entity suppressed the alarms during business hours. This violation began on July 1, 2016, when the Standard and I on when the entity turned on the forced entry and door held open alarms during business hours, for a total of days of WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instal a physical access point into three PSPs and issue an alarm or alert in response to detected unauthorized access through a physical access through a ph							
			Security Incident response plan within 15 minutes of detection, as required by CIP-006-6 R1 Parts 1.4 and 1.5. Such failure could potentially result in an attacker gaining access to critical systems without the entity's knowledge, prolonging the time the a them to escape undetected. An attacker could also monitor, manipulate, or disable Cyber Assets without entity knowledge. However, as con one of the PSPs was equipped with a camera to observe the interior of the room.							
Mitigation			 To mitigate this violation, the entity has: activated alarms for existing forced entry and door held open alarms during business hours; updated its technician procedure for testing physical security mechanisms to include language from the Standard as a reminder of door forced open and held open alarms are always communicated to the System Operators; and provided training to its technical personnel on what is required for compliance with CIP-006-6 R1 and the updated procedure. 							
Other Factors			These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WECC posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the d Agreement with a \$0 penalty. WECC considered the entity's compliance history and determined there were no relevant instances of noncompliance.							

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation					
npliance Audit	11/6/2018	08/19/2019					
ree PSPs controlli	ng access to MIBCSs,	, the entity was unable to					
t 1.4 and alarms or alerts in response to detected unauthorized							
o within 15 minut	es of detection as rea	uired by CIP-006-6 B1 Part					
	es of detection as req						
vere manned, no monitoring or automated alarming or alerting Requirement became mandatory and enforceable, and ended noncompliance.							
nce, the entity failed to monitor for unauthorized access through							
point into said PSPs to the personnel identified in the BES Cvber							

e attacker could use for nefarious purposes and possibly allow ompensation the PSPs were manned and and

the requirements for compliance which includes verifying that

C2018018977, WECC2018019483, and WECC2017018365) disposition treatment to an Expedited Settlement

NOC-2658

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
WECC2017017911	CIP-007-6	R2: P2.3	Medium	Medium Severe 10/01/2016 05/09/		05/09/2017	5				
Description of the Violat document, each violatio "violation," regardless o and whether it was a po violation.)	tion (For purpose n at issue is desc f its procedural p ssible or confirm	s of this ribed as a posture ed	On July 7, 2017, the entit in potential noncomplian Specifically, on August 2 conversion of its network However, the entity did n without incident, for a to	cy submitted a Self-Report st nee with CIP-007-6 R2. The Cy 6, 2016, the entity evaluate from switching to routing, it not create a dated mitigation stal of 221 days of noncompl	ating, as a year of the security patch as applicable to a security patch as applicable to a security patch as applicable to a security patch and plan within 35 calendar days of the eviance.	th the entity's MIBCS located EACMS which it planned to install on the EACMS without interrupting se valuation completion as required by Pa	by Sept ervice to art 2.3.				
			The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2 was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the experiencing a server hardware failure which required the software to be installed on different hardware delaying the evaluation of securi								
Risk Assessment			WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this inside the series of the evaluation completion for one security patch identified as applicable to EACMS and failed to apply one application completion, as required by CIP-007-6 R2 Part 2.3. Such failures could have prolonged the presence of software vulnerabilities, which if exploited, could allow unauthorized access to or misure However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant of guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physicates the provide the presence of physicates access to physicates access to physicate these violations.								
detect these violations. Mitigation To mitigate this violation, the entity has: 1) evaluated security patches released since the previous evaluation; 2) installed the applicable security patch. 3) provided additional training to technical staff on security patching activities; 4) implemented an internal control to daily back-up the server and provide an alert to technical staff on the process for creating a mitigation 6) trained technicians on the new process; 7) created an annual task to review the patch management program with technicians to reinforce 8) updated its patch management program with language stating that upon determination of the amonth from the day of applicability determination; 9) changed the email task reminders from being sent to just the technicians but also to management to ensure the task is completed; and						echnical staff with the status of the band mitigation plan when a security patch of o reinforce the entire patch management fon of the applicability of a patch, a chan management staff and the state of the security s and management as an additional co	ack-up; cannot k ent prog inge req				
Other Factors			WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevant indicative of broader compliance issues.								

		_								
od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation								
Self-Report	09/21/2018	10/08/2019								
		it was								
tember 30, 2016. Due to installation issues during the entity's its distribution Supervisory Control and Data Acquisition system. On May 9, 2017, the entity was able to install the security patch										

2) less than adequate patch management procedure in that it e stated date, and 3) software being used to track patches rity patches for applicability.

istance, the entity failed to create a dated mitigation plan within icable security patch to BCAs within 35 calendars days of the

use of Cyber Assets that impact the reliability of the BPS. . communication with the technicians, giving them verbal ical access. The entity did not implement controls to prevent or

be installed;

gram;

uest shall be created that same day with a due date one calendar

, who will escalate past-due tasks to supervisors and follow-up

ant history was an issue in 2014 that posed minimal risk and not

		-									
NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
WECC2018018977	WECC2018018977 CIP-007-6 R2: P2.3		Medium	Severe	Severe 09/29/2017		S				
Description of the Violat document, each violatio "violation," regardless o and whether it was a po violation.)	tion (For purpose n at issue is desc f its procedural p ssible or confirm	es of this ribed as a posture ed	On January 12, 2018, the it was in potential nonco Specifically, for the first was installed on second instance, on Aug June 24, 2017, and again required by Part 2.3. Ho The causes of this violat was not clear who was re experiencing a server has	it was in potential noncompliance with CIP-007-6 R2. The Cyber Assets in scope were associated with the entity's MIBCS located Specifically, for the first instance, on August 24, 2017, the entity evaluated a security patch as applicable to EACMS which it planned to and performing cyber vulnerability assessments, the installation of the security patch was overlooked, and no tim was installed on of the EACMS on December 20, 2017, and a mitigation plan was created for the remaining EACMS on December second instance, on August 16, 2017, the entity evaluated a security patch as applicable to EACMS which was outside of the 35 calend June 24, 2017, and again, the entity applied the security patch on January 2, 2018, for a total of 96 days of noncompliance. The causes of this violation were attributed to: 1) a lack of controls to escalate security patch reminder emails that were not acted upon, 2 was not clear who was responsible for creating a mitigation plan or how the mitigation plan would be tracked to ensure completion by the experiencing a server hardware failure, which required the software to be installed on different bardware delaying the evaluation of security patch							
Risk Assessment			WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these in 35 calendar days of the evaluation completion for one security patch identified as applicable to EACMS and failed to apply one applied evaluation completion, as required by CIP-007-6 R2 Part 2.3. Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misur However, as a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant guidance on the issue during the noncompliance. Additionally, the PACS resided within an ESP and PSP with restricted electronic and physidetect these violations.								
Mitigation			To mitigate this violation 1) evaluated secur 2) installed the app 3) provided addition 4) implemented ard 5) updated its pate 6) trained technici 7) created an annu 8) updated its pate month from the 9) changed the emto ensure the tat 10) implemented er	n, the entity has: ity patches released since the plicable security patch. onal training to technical staf n internal control to daily bac ch management program to c ans on the new process; ual task to review the patch m ch management program with e day of applicability determin nail task reminders from being task is completed; and mailing reports of due or past	e previous evaluation; f on security patching activities; k-up the server and provide an aler learly define the process for creatin nanagement program with technician language stating that upon determ nation; g sent to just the technicians but al	t to technical staff with the status of t ng a mitigation plan when a security pa ans to reinforce the entire patch mana nination of the applicability of a patch, so to management staff and the gnees and management as an addition	he back-up; atch cannot b gement prog a change requ				
Other Factors			These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WEC posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the Agreement with a \$0 penalty. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevan indicative of broader compliance issues.								

Western Electricity Coordinating Council (WECC)

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
Self-Report	10/05/2018	10/10/2019
o install by Septen ely action was tal er 21, 2017, for a dar day window fr beyond the 35 cal	nber 28, 2017. Howev ken as required by Pa duration of 84 days o rom the previous eval endar days since the	er, rt 2.3. The security patch f noncompliance. For the uation which occurred on evaluation completion, as
2) less than adequ e stated date, and rity patches for ap	iate patch manageme I 3) software being us oplicability.	ent procedure in that it ed to track patches
stances, the entit	y failed to create a da	ted mitigation plan within
cable security pat	ch to BCAs withi	n 35 calendars days of the
se of Cyber Asset communication w ical access. The e	s that impact the relia with the technicians, g entity did not impleme	ability of the BPS iving them verbal ent controls to prevent or
be installed;		
gram; quest shall be crea	ted that same day wit	h a due date one calendar:
, who will escal	ate past-due tasks to	supervisors and follow-up
ECC2018018977, e disposition trea	WECC2018019483, a tment to an Expedite	nd WECC2017018365) d Settlement
nt history was an	issue in 2014 that po	sed minimal risk and not

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level Violation Start Date		Violation End Date	Metho			
WECC2018019483	CIP-007-6	R2: P2.2 Medium		Lower	01/31/2018	02/01/2018	S			
Description of the Violat document, each violatio "violation," regardless o and whether it was a po violation.)	tion (For purpose n at issue is desc f its procedural p ssible or confirm	s of this ribed as a posture ed	On April 5, 2018, the ent was in potential noncom Specifically, on Decembe once every 35 calendar of The causes of this violati was not clear who was re experiencing a server ha	ity submitted a Self-Report sipliance with CIP-007-6 R2. The 26, 2017, the entity evaluated ays, per Part 2.2, which show on were attributed to, 1) a latesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired which required to the statesponsible for creating a mitired	tating that as a second second secon	ed with the entity's MIBCS located e next evaluation did not occur until Fo otal of two days of noncompliance. In reminder emails that were not acted would be tracked to ensure completion ent hardware delaying the evaluation of	ebruary upon, 2 on by the of securi			
Risk Assessment			WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In these inservaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1 Such failures could have prolonged the presence of software vulnerabilities, which if exploited could allow unauthorized access to or misus attacker gained access to a PACS, they could deny PSP access to authorized personnel or allow entry to unauthorized persons. The PSP con attacker to manipulate, disable, or destroy Cyber Assets critical to the BPS. However, as a corrective control for the BCAs and EACMS in second in constant communication with the technicians, giving them verbal guidance on the issue during the noncompliance. Additionally, the PAC physical access. The entity did not implement controls to prevent or detect these violations.							
Mitigation			To mitigate this violation 1) evaluated securi 2) installed the app 3) provided additio 4) implemented an 5) updated its patch 6) trained technicia 7) created an annu 8) updated its patch month from the 9) changed the emain to ensure the tass 10) implemented emain 10	h, the entity has: ty patches released since the plicable security patch. anal training to technical staff internal control to daily back h management program to c ans on the new process; al task to review the patch m h management program with day of applicability determin ail task reminders from being sk is completed; and hailing reports of due or past	e previous evaluation; ² on security patching activities; k-up the server and provide an alert to t learly define the process for creating a n nanagement program with technicians t language stating that upon determination ation; g sent to just the technicians but also to due change request tickets to assignee	technical staff with the status of the ba mitigation plan when a security patch o o reinforce the entire patch managem ion of the applicability of a patch, a cha o management staff and the security s and management as an additional co	ack-up; cannot k ent prog ange requ			
Other Factors			These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911, WEC posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in scope, WECC escalated the Agreement with a \$0 penalty. WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous relevar and not indicative of broader compliance issues.							

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation								
Self-Report	05/21/2019	10/09/2019								
		, it								
1, 2018, which was beyond the requirement to evaluate at least										
 less than adeque stated date, and rity patches for approximation 	ate patch manageme 3) software being us pplicability, respective	ent procedure in that it ed to track patches ely.								
stances, the entit .1 for PACS	y failed to at least on , as required by CIP-0	ce every 35 calendar days, 07-6 R2 Part 2.2.								
se of Cyber Assets that impact the reliability of the BPS. If an ntrolled access to the MIBCS that if compromised could allow an cope, the entity ensured that the Control Systems engineer was CS resided within an ESP and PSP with restricted electronic and										
be installed; gram; quest shall be crea	ted that same day wi	th a due date one calendar								
, who will escal	ate past-due tasks to	supervisors and follow-up								
CC2018018977, V e disposition trea	VECC2018019483, an tment to an Expedite	d WECC2017018365) d Settlement								
nt history consist	ed of an issue in 2014	l that posed minimal risk								

NOC-2658

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method o Discovery				
WECC2017018365	CIP-007-6	R4: P4.2; Sub-part 4.2.2	Medium	High	07/01/2016		Complia				
Description of the Violat	tion (For purpose	es of this	During a Complian	uring a Compliance Audit conducted , WECC determined the entity, as a							
document, each violatio	n at issue is desc	cribed as a			, was in potential noncompliance w	ith CIP-007-6 R4 Part 4.2 sub-part 4.2	.2. Specifica				
"violation," regardless o whether it was a possibl	f its procedural le or confirmed v	posture and /iolation.)	event logging on	BCAs, EACMS, and	PACS associated with the MIBCS lo	cated at					
			After reviewing all relevant information, WECC Enforcement concurs with the audit finding as stated above. The root cause was attributed designed to weed out false positives was in fact suppressing alerts for failed logins not associated with two-factor authentication. This Requirement became mandatory and enforceable to the entity, and ended on August 29, 2017, when logging of detected failures was decommissioned, for a total of 425 days of noncompliance.								
Risk Assessment			WECC determined this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this that included detected failure of event logging for BCAs, EACMS, and PACS associated with the MIBCS located at 007-6 R4 Part 4.1 sub-part 4.2.2.								
			The entity did not implement controls to detect or prevent this violation. However, as compensation the entity was able to collect lo a corrective control for the BCAs and EACMS in scope, the entity ensured that the Control Systems engineer was in constant commu- issue during the noncompliance. The PACS resided within an ESP and PSP with restricted electronic and physical access.								
Mitigation			To remediate and mitigate this violation, the entity has:								
			1) updated th	ne Windows auditing config	uration and the SIEM alert rule which e	enabled alerting for detected failure o	of event logg				
			2) updated its technician procedure to include more detail on configuring the Windows auditing section; and								
			3) completed initial and annual testing to ensure the SIEM is receiving and alerting on login attempts for the Cyber Assets in sco								
Other Factors			These violations (WECC2017017507, WECC2017017631, WECC2017017632, WECC2017017633, WECC2017017634, WECC2017017911 WECC2017018365) posed a minimal risk to the reliability of the BPS. However, due to the number of violations and Cyber Assets in set Expedited Settlement Agreement with a \$0 penalty.								
			WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because the previous re risk and not indicative of broader compliance issues.								

of /	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation								
ance Audit	11/07/2018	10/09/2019								
ally, the entity failed to generate alerts for the detected failure of										
buted to a design failure in that one of the rule building blocks is violation began on July 1, 2016, when the Standard and is enabled on six of the Cyber Assets, and one Cyber Asset was										
is instance, th	e entity failed to generate	e alerts for security events as required by CIP-								
gs locally eve nication with	n though alerting was not the technicians, giving the	enabled. Additionally, as m verbal guidance on the								
ging for Cyber Assets, and decommissioned one Cyber Asset;										
1 WECC2018		R and								
scope, WECC	escalated the disposition t	reatment to an								
elevant histo	ry consisted of an issue in	2014 that posed minimal								

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					
WECC2017017676	CIP-002-5.1	R1, P1.1, P1.2	High	Lower	7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity)	3/15/2019 (when the entity completed mitigating activities)	Self-Report	3/15/2019	4/2/2019					
Description of the Viola	ation (For purpos	ses of this	On May 30, 2017, the e	ntity submitted a Self-Repor	rt stating that, as a				, it was in					
document, each violati	on at issue is des	scribed as a	violation of CIP-002-5.1 F	R1.										
"violation," regardless	"violation," regardless of its procedural posture and													
whether it was a possib	ole or confirmed	violation.)	Specifically, on March 8,	2017 during the planning ar	nd engineering activities associated w	vith upgrading tone telemetry equipr	ment at the	Control Center	the entity discovered					
			that Remote Terminal Unit (RTU) was not considered per CIP-002-5.1 R1; therefore, the RTU was not identified as a High Impact BES Cyber System (HIBCS) per CIP-002-5.1 R1 Part 1.1. The RTU											
			was subsequently evaluated, through the entity's established BES Cyber Asset identification process, as being a Cyber Asset. The RTU was classified as a BES Cyber Asset (BCA) associated with a HIBCS,											
			since the RTU resided in	a facility containing HIBCS.										
			The entity determined that the RTU should be classified as a BES											
			Cyber Asset, due to its ro	Cyber Asset, due to its role in the second s										
			entity. In addition, the er	ntity had an increase in scope	e from what it originally Self-Reported	d. During mitigation of the violation, t	the entity discovered	more RTUs that it fai	led to correctly identify as					
			part of its Medium Impa	ct BES Cyber Systems (MIBC	S) located at several of its substation	ns. Regarding the scope increase of	RTUs; the entity had i	ncorrectly identified	of the RTUs as non-CIP					
			devices; of the RTUs	were assessed as having the	e incorrect impact rating; and of t	he RTUs were missing in the initial in	nventory and therefore	were never identifie	d. WECC determined that					
			because these devices w	ere BCAs within a HIBCS and	MIBCS, the entire suite of CIP Standa	ards and Requirements should be app	olied to these devices	s, as applicable.						
			RIUs as a start of the HURCS and MURCS.											
			part of its HIBCS and WIB											
			The root cause of the noncompliance was less than adequate process for properly considering each of its assets for purposes of identify the impact rating of RES (wher Systems at each asset											
			Specifically, since the RT	Us were utilized as		, the entity believed they we	re non-BES assets. and	therefore did not incl	ude them in the initial 15-					
			minute impact analysis.	minute impact analysis										
			This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable on the entity, and ended on March 15, 2019, when the entity completed mitigating activities, for a total of 988 days of noncompliance.											
Risk Assessment			WECC determined this v	iolation posed a moderate ri	sk and did not pose a serious or subst	tantial risk to the reliability of the bu	lk power system BPS. In	this instance, the en	tity failed to appropriately					
			identify and protect RTUs associated with its HIBCS and MIBCS, as required by CIP-002-5 R1 Part 1.1 and 1.2.											
			Such failure could have r	esulted in the compromise c	of the RTUs, any adjacent Cyber Assets	s, and the associated HIBCS or MIBCS	; to include gaining con	nplete control of the I	3CAs which could have led					
			to misconfigurations, inv	alid data being sent, introduc	ction of malicious firmware or lock-out	t of the BCAs; thereby potentially affe	ecting the reliability and	security of the BPS. H	owever, as compensation,					
			the RTUs were serially co	onnected and as such had no	o routable network connectivity; base	eline configuration information was r	maintained on the RTU	s; the RTU that sh	ould have been classified					
			and protected as a HIBCS	did not provide control fun	ctions and was configured to only trar	nsmit, not receive, data; and the othe	er RTUs that should h	nave been classified a	nd protected as MIBCS did					
			not have control capabili	not have control capabilities. All RTUs had the protective measures of CIP-007-6 applied, as verified by WECC.										
				—										
Mitigation			To remediate and mitiga	te this violation, the entity h	as:									
			1) correctly identifi	ed and documented the	RTUs in scope;									
			2) verified whether the RTUs were compliant with applicable CIP Standards and Requirements, and where they were not, applied the necessary protective measures of the CIP Standards and											
			Requirements,											
			3) identified eight g	gaps in its control design and	control operations;									
			4) worked with stakeholders to address the identified gaps;											

Western Electricity Coordinating Council (WECC)

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		
WECC2017017676	CIP-002-5.1	R1, P1.1, P1.2	High	Lower	7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity)	3/15/2019 (when the entity completed mitigating activities)	Self-Report	3/15/2019	4/2/2019		
	 5) updated its process, procedures, and controls; 6) communicated changes to its Change Advisory Board; and 7) provided awareness and training to applicable individuals within its organization. 										
Other Factors	ther Factors WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. WECC considered the entity's CIP-002-5.1 R1 compliance history to be an aggravating factor in the penalty determination.										

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Compliance Exceptions in this posting and provide
the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	NPCC2018019849	Yes		Yes	Yes						Yes			Categories 3 – 4, 10: 2 years Category 1: 3 years
2	NPCC2018019848	Yes		Yes	Yes						Yes			Categories 3– 4, 10: 2 years Category 1: 3 years
3	NPCC2018019847	Yes		Yes	Yes						Yes			Categories 3– 4, 10: 2 years Category 1: 3 years
4	NPCC2018019846	Yes		Yes	Yes						Yes			Categories 3– 4, 10: 2 years Category 1: 3 years
5	NPCC2018019845	Yes		Yes	Yes						Yes			Categories 3– 4, 10: 2 years Category 1: 3 years
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														

Filing Date: October 31, 2019

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		
NPCC2018019849	CIP-005-5	R1.	Medium	VSL - Severe	7/1/2016	6/6/2018	On-site Audit	9/6/2018	7/31/2019		
Description of the Violat	ion (For purposes	s of this	During a Compliance Audit	conducted from	NPCC determined	that (the entity), as a	W	as in noncompliance v	vith CIP-005-5 R1 (1.3).		
document, each violatio	n at issue is descr	ibed as									
a "violation," regardless	of its procedural		This violation started on Jul	ly 1, 2016, when the entity f	failed to identify the reason for grant	ng inbound and outbound access permis	sions on Electronic Acce	ss Points for one Med	ium Impact BES Cyber		
posture and whether it v confirmed violation.)	Examples for and and and and and and and and access permissions and up firewall rules.							ssions and updated its			
Specifically, several firewall rules within two (2) Medium Impact EACMS that provide Electronic Access Points to Medium Impact BES Cyber Systems did not have valid permission. There were rules with an "unknown" reason as well as rules that were no longer necessary.								nave valid reasons for	granting the access		
The root cause of this violation was the lack of regular review and an undue reliance on a single person. Previous to the NERC CIP Audit, the review of firewall rules was who was unable to spend the necessary time on this type of review. The entity is now reviewing the firewall rules as a team and completing the reviews at least quarter								ll rules was the respo ast quarterly.	nsibility of one person		
Risk Assessment			he violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Unnecessary EAP rules and active firewall rules where the reason for granting access is unknown can provide paths into the Electronic Security Perimeter (ESP) that can be exploited to gain unauthorized entry.								
The entity has several systems in place to detect and prevent a potential incident. While some of the entity's firewall rules had been marke firewall did have rules enabled to restrict access to and from the ESP. The entity also						n marked as unknown bu	siness reason or mark	ed as to be removed, the			
			No harm is known to have o	occurred as a result of this v	violation.						
Mitigation			To mitigate this violation, the second s	he entity							
			 Reviewed and update 	ated its Firewall rules; and							
			Initiated a process	to review vulnerability asse	ssment action plans quarterly that inc	ludes additional staffing					
Other Factors			NPCC reviewed the entity's	internal compliance progra	am (ICP) and considered it to be a neu	tral factor in the penalty determination.					
			NPCC considered the entity	's compliance history and d	letermined there were no relevant in	tances of noncompliance.					

\$84,000

NERC Violation ID	Reliability	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Meth
	Standard	-					
NPCC2018019848	CIP-005-5	R2.	Medium	VSL - Moderate	11/18/2016	6/7/2018	On-sit
Description of the Violat	tion (For purpose	es of this	During a Compliance Audit	conducted from	NPCC determined th	at (the entity), as a	
document, each violatio	n at issue is desc	ribed as					
a "violation," regardless	of its procedura	I	This violation started on N	ovember 18, 2016, when the	entity failed to utilize an Intermediate	System such that the Cyber Asset initi	ating Int
posture and whether it	was a possible, o	or	Medium Impact BES Cyber	Assets. The violation ended	on June 7, 2018, when the entity disable	led the interactive remote access. How	vever, th
confirmed violation.)							
			The root cause of this viola	ation was misinterpretation of	of both the standard and the recommer	nded solutions provided by NERC.	
Risk Assessment	sk Assessment		The violation posed a mod	erate risk and did not pose a	serious or substantial risk to the reliab	ility of the bulk power system. Specifie	cally, fai
			with additional vectors to	attack the entity's Medium I	mpact BES Cyber Systems and gain unau	uthorized access.	
				• • • • • • • •			
			The entity reduced the risk	c of an individual gaining una	uthorized access		
			M/hilo the entity is mitigati	ng the violation			
			while the entity is mitigati	ng the violation,			
			No harm is known to have	occurred as a result of this w	iolation		
Mitigation			To mitigate this violation	the entity.			
WithBatton			1) Disabled VPN conr	and children and c			
			2) Designed along w	ith a third-party vendor, a ne	w Interactive Remote Access Solution a	as an alternate system to meet the req	uiremer
			3) Implemented the	new Interactive Remote Acce	ess Solution.		10
Other Factors			NPCC reviewed the entity'	s internal compliance progra	m (ICP) and considered it to be a neutra	al factor in the penalty determination.	
				· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		
			NPCC considered the entit	y's compliance history and d	etermined there were no relevant insta	nces of noncompliance.	

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
e Audit	12/10/2018	7/31/2019
, wa	is in noncompliance v	vith CIP-005-5 R2 (2.1.).
eractive Remote	Access does not dired	ctly access the entity's
lure to utilize an l	ntermediate System	can provide attackers
nts, and		

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
NPCC2018019847	CIP-007-6	R2.	Medium	VSL - Severe	7/1/2016	7/19/2018	On-site Audit	11/28/2018	7/31/2019
Description of the Violat document, each violatio	tion (For purposes on at issue is descr	s of this ribed as	During a Compliance Audit	conducted from	NPCC dete	rmined that (the entity), as a	wa	as in noncompliance v	vith CIP-007-6 R2. (2.1.).
a "violation," regardless posture and whether it confirmed violation.)	of its procedural was a possible, o	r	This violation started on Jul added the three (3) Mediur	y 1, 2016, when the entity f n Impact BES Cyber System: three unmanaged switches :	tailed to include three (3) Med s to its patch tracking spreads that are classified as Medium	dium Impact BES Cyber Systems in its patch heet and reviewed software updates for ap	management process. The vie plicability. racking or evaluating security	plation ended on July	19, 2018, when the entity
			The root cause of this violat	ements.		, wh	ich led to the exclusion of		
Risk Assessment			The violation posed a minin leave the devices vulnerabl entity's operators would los by not configuring these sw	nal risk and did not pose a s e to known exploits and cou se the ability to remotely co vitches to use a routable pro	erious or substantial risk to th uld provide a bad actor the ab ontrol the SCADA system. The otocol.	ne reliability of the bulk power system. Spec ility to gain unauthorized access to the Elec e entity in this instance reduced the risk of a	ifically, not evaluating applica trionic Security Perimeter. If t n attacker identifying a know	able systems for cyber the switches in scope n unpatched exploit c	security patches could were taken offline, the in the switches in scope
			If an attacker or expoit wer released for the switches in No harm is known to have o	e to take the devices offline scope and determined the occurred as a result of this v	e, the entity y were not applicable. violation.	. Aft	er the issue was discovered, t	he entity evaluated t	ne patches that had been
Mitigation			To mitigate this violation, the second secon	ne entity: hecklist to include a check f e; and 107-6 Standard and its 100 p	for firmware; rocess Documentation.				
Other Factors			NPCC reviewed the entity's NPCC considered the entity	internal compliance progra 's compliance history and d	im (ICP) and considered it to t letermined there were no rele	be a neutral factor in the penalty determinates a neutral factor in the penalty determinates of noncompliance.	ion.		

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
NPCC2018019846	CIP-007-6	R5.	Medium	VSL - Severe	7/1/2016	9/28/2018	On-site Audit	10/17/2018	7/31/2019
Description of the Violat	ion (For purpos	es of this	During a Compliance Audit	conducted from	, NPCC determined th	at (the entity), as a	wa	s in noncompliance v	with CIP-007-6 R5. (5.4).
document, each violatio	n at issue is des	cribed as							
a "violation," regardless	of its procedura	al	This violation started on Ju	ly 1, 2016, when the entity f	failed to change known default passwor	ds on 45 Medium Impact Cyber Assets	The violation ended on	September 28, 2018,	when the entity changed
posture and whether it	was a possible,	or	the known default passwor	rd on applicable cyber assets	s that are capable of having a password	set.			
confirmed violation.)									
			The root cause of this viola	tion was failure to impleme	nt CIP Standard Requirements based or	n mitigating factors.			
			Specifically, the entity chose	se not to change passwords	on the 45 applicable systems due to the	e following mitigating factors: substation	ns do not have External	Routable Connectivit	у.
Risk Assessment	Risk Assessment			mal risk and did not pose a s	erious or substantial risk to the reliabili	ty of the bulk power system. Specifical	y, unchanged known de	fault passwords can p	provide attackers with
			unauthorized access to app	blicable Cyber Assets.					
			The entity reduced the rick	of an unauthorized individu	al loveraging a known default passwor	to access the 45 substation relays in s	cono hy implementing a	multi lavorad cocurit	w approach
			The entity reduced the risk		iai levelaging a known delauit password	a to access the 45 substation relays in s	cope by implementing a	multi-layered securit	у арргоаст.
			No harm is known to have	occurred as a result of this v	violation				
Mitigation			To mitigate this violation, t	he entity:					
			1) Changed password	ls for the assets in scope: an	d				
			2) Updated its NERC	CIP Training Program to inclu	ude a reminder that all BCAs must have	their default/manufacturer password of	changed before a BCA is	put into service.	
Other Factors			NPCC reviewed the entity's	s internal compliance progra	m (ICP) and considered it to be a neutro	al factor in the penalty determination.	0		
					(- ,				
			NPCC considered the entity	y's compliance history and d	etermined there were no relevant insta	inces of noncompliance.			

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation		
NPCC2018019845	CIP-010-2	R3.	Medium	VSL - Severe	7/1/2016	6/6/2018	On-site Audit	9/6/2018	7/31/2019		
Description of the Violat document, each violatio a "violation," regardless posture and whether it confirmed violation.)	ion (For purpose n at issue is desc of its procedural vas a possible, o	s of this ribed as r	During a Compliance Audit This violation started on Ju vulnerabilities identified in the mitigation plans. Specifically, the entity com items, the subject matter e The root cause of this viola	During a Compliance Audit conducted from was in noncompliance with CIP-010-2 R3 (3.4). This violation started on July 1, 2016, when the entity failed to document the planned date of completion of the action plan and/or the execution status of the mitigation plans it created to mitigate vulnerabilities identified in its CIP-010-2 R3 vulnerability assessments. The violation ended on June 6, 2018, when the entity documented the completion date of the action plans and/or execution status of the mitigation plans. Specifically, the entity completed its 2018 Cyber Vulnerability Assessment (CVA), but did not document the planned completion date and/or status of each of the CVA findings. Additionally, for many items, the subject matter experts were unsure of the status/planned completion date.							
Risk Assessment			responsibility of one person and updates occurs at least The violation posed a mode attacker a vector to take ac There were 40 items open items did not have a docun . Some of the vulnerab The entity reduced the risk	n who was unable to spend to quarterly. erate risk and did not pose a lvantage of technical flaws a on the entity's mitigation pla nented status and action. Th ilties to be mitigated include of having systems with know	the necessary time on this responsibility serious or substantial risk to the reliabil and configuration errors, which could all an, some of the items were out of scope le items impacted one Medium Impact E ed: wn vulnerabilities within its Electronic Se	. The oversight of vulnerability asses ity of the bulk power system. Specif ow an attacker to gain control of on of NERC CIP, and many items were SES Cyber System that is associated v ecurity Perimeter (ESP) by	issments is now the respon ically, allowing vulnerability e Medium Impact BES Cyb security improvements ve with System Operations	sibility of a team and res to go unmitigated er System. rsus vulnerabilities. Fi	completing the review could provide a potential ve (5) of the forty (40)		
Mitigation			To mitigate this violation, t 1) Updated its mitigat 2) Initiated a process	he entity: ion plans before the audit w to review vulnerability asses	vas complete; and ssment action plans quarterly that includ	led additional staffing.					
Other Factors			NPCC reviewed the entity's NPCC considered the entity	internal compliance progra 's compliance history and d	m (ICP) and considered it to be a neutra etermined there were no relevant insta	I factor in the penalty determination nces of noncompliance.	1.				

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	TRE2016016184	Yes		Yes	Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 year

Filing Date: September 26, 2019

Last Updated 09/26/2019

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
TRE2016016184	CIP-002-5.1	R1	High	Lower	7/1/2016 (when the Standard became mandatory and enforceable)	Present	Self-Certification	11/7/2019 (approved completion date)	TBD
Description of the Viol	ation (For nurno	ses of this	On	the Entity submitted a Self-	Certification stating that as a		it was in no	ncompliance with Cl	P-002-5 1 B1 Specifically
document, each violat "violation," regardless	ion at issue is de of its procedura	scribed as a l posture and	the Entity did not have o BES Cyber System. This is	r implement a process that ssue began when CIP-002-5.1	considers Example for the purpos 1 became enforceable and continued	es of CIP-002-5.1 R1, Parts 1.1 tl I after CIP-002-5.1a R1 became e	hrough 1.3. As a result, the E enforceable.	ntity did not identify	each asset that contains a
			The root cause of this iss Entity did not document	ue is that the Entity did not h or implement processes nec	nave any documented process for co cessary for compliance with CIP-002-	mpliance with CIP-002-5.1 durinរ 5.1.	g the period leading up to CIP	-002-5.1 becoming er	forceable. As a result, the
			This noncompliance start	ted on July 1, 2016, when CIF	P-002-5.1 R1 became enforceable an	d is currently ongoing.			
Risk Assessment			This issue posed a moder increases the potential th CIP-002-5.1 became enfo	ate risk and did not pose a se at the BES Cyber System wil prceable, until the present. I	erious or substantial risk to the bulk I not receive the appropriate cyber s In addition, during the noncomplian In addition, the Entity's initial	power system based on the follo ecurity protections. The duration ce, the Entity's	owing factors. The failure to p n of this issue was approxima at the Entity	roperly identify and c tely three years, lastir	assify a BES Cyber System Ig from July 1, 2016, when BES Cyber
Mitigation			To mitigate the noncomp	Jiance, the Entity:	002 E 12, which includes a prolimina	u draft of the identifications rea	wired by CIP 002 E 12 P1		
			 approved a documer established a complia process for identifyir 	nted internal compliance with CP-0 ance committee, as describe ag applicable Reliability Stand	pram, which includes a prelimital gram, which includes a process for i d in the documented internal compl dards; and	dentifying applicable current and iance program, which determine	d new Reliability Standards; es upcoming deadlines at regu	ular meetings and imp	plements the Entity's
			4) conducted training re	egarding the Entity's process	for compliance with CIP-002-5.1a a	nd regarding the Entity's overall	compliance program.		
			Furthermore, the Entity s	submitted a Mitigation Plan f	to address the following actions that	will be completed by November	r 7, 2019:		
			1) finalize and have CIP	Senior Manager approve the	e draft identifications required by CI	P-002-5.1a R1.			
			The Entity requires for compliance with CIP-	002-5.1a R1.			and intends to comp	blete this change befo	re finalizing its process
Other Factors			Texas RE considered the	Entity's compliance history a	and determined there were no releva	ant instances of noncompliance.			

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	MRO2017018152	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 - 12: 2 years
2	MRO2017018150	Yes		Yes	Yes						Yes			Category 1: 3 years; Category 2 - 12: 2 years

Filing Date: August 29, 2019

("the	Entity")
-------	----------

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc		
MRO2017018152	CIP-007-6	R5.7	Medium	Severe	7/1/2016 (when the Standard became mandatory and enforceable)	10/31/2018 (when all applicable Cyber Assets were configured to either lockout or send a real-time alert)	Com		
Description of the Viola document, each violatio "violation," regardless o whether it was a possib	tion (For purpos on at issue is des of its procedural lle, or confirmec	es of this cribed as a posture and violation.)	During a Compliance Audi w not configured to either li The cause of the noncomp Exception (TFE) if the devi attempts, and failed to co	it conducted from CIP-007-6 mas in violation of CIP-007-6 mit the number of unsucces pliance was the Entity's failu ice could not meet the requinsider a device's event forv	, MRO det R5. Sampling conducted during the Co ssful authentication attempts or gene ure to understand the full scope of the irements. Additionally, the Entity only varding capability in conjunction with	termined that the Entity, as a second ompliance Audit and a subsequent ex rate alerts after a threshold of unsuce e Standard and Requirement. The Ent y considered whether a device had th a collection system(s) that can gener	itent of cessful ity bel ie capa ate an		
Risk Assessment			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Two noncompliance. One of the devices had a low inherent risk to the BPS as it was a terminal server that transferred redundant informati receiving some level of protection at the time of the Compliance Audit. Prior to the audit, event forwarding had been turned on for th report (MRO does not consider an alert from an hourly report to be compliant with P5.7). Finally, the Entity's No harm is known to have occurred.						
Mitigation			To mitigate this violation, 1) submitted a TFE for two 2) conducted an extent of 3) configured all applicabl 4) augmented the account 5) validated updated proc	the Entity: o devices; condition review; e devices to either lockout t implementation form to a sess and provided training to	or send a real-time alert; dd additional steps and permit the ele o SMEs through a table top exercise o	evation of concerns for peer or super f actual assessment of applicable Cyb	visory per Ass		
Other Factors			 MRO considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance should be self-detected through internal controls. However, MRO determined that even though the noncompliance should not be elig does not warrant a financial penalty given the minimal impact of the noncompliance upon the BPS. MRO considered the Entity's CIP-007-6 R5 compliance history in determining the penalty. MRO determined that the Entity's compliance was not warrant be prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not warrant be penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance did not involve noncompliance with P5.7 and the current noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the prior instances of noncompliance was not penalty because the penalty because						

thod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
npliance Audit	2/25/2019	2/25/2019

f condition analysis uncovered multiple Cyber Assets that were I authentication attempts, as required by P5.7.

lieved that it was not required to file a Technical Feasibility ability to limit the number of unsuccessful authentication a alert as a method for complying with P5.7.

of the devices were granted a TFE that resolved the cion to map boards. The majority of remaining devices were nese devices, which were configured to alert through an hourly

review; and set(s).

iance that impacts a high population of applicable devices gible for Compliance Exception treatment, the noncompliance

nce history should not serve as a basis for aggravating the not caused by a failure to mitigate the prior noncompliance.

MRO2017018150 CIP-010-2 R1.1.2 Medium Lower 7/1/2016 (when the Standard became mandatory and enforceable) 5/11/2018 (updated the existing baselines to include all intentionally installed software) Compliance Audit 2/25/2019 2/25/2019 Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.) During a Compliance Audit conducted from software it included all installed commercially available software as required by P1.1. The Entity did not include the software on the documented baseline for two was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber version that was installe	yber Assets that did two devices and the system (an alternate ool. The software er Asset. The Entity ssible discrepancies.										
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.) During a Compliance Audit conducted from	yber Assets that did two devices and the t system (an alternate pol. The software per Asset. The Entity ssible discrepancies.										
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.) During a Compliance Audit conducted from to conducted from to compliance Audit conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber not have baselines that included all installed commercially available software as required by P1.1. The Entity did not include the software on the documented baseline for two tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber is included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber is did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible	yber Assets that did two devices and the t system (an alternate pol. The software per Asset. The Entity ssible discrepancies.										
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.) During a Compliance Audit conducted from the compliance Audit and a subsequent extent of condition analysis uncovered multiple Cybe control and the compliance Audit and a subsequent extent of condition analysis uncovered multiple Cybe control and the compliance Audit and a subsequent extent of condition analysis uncovered multiple Cybe control and the baselines that included all installed commercially available software as required by P1.1. The Entity did not include the control and the baseline tool or its patch management system tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible	yber Assets that did two devices and the t system (an alternate col. The software per Asset. The Entity ssible discrepancies.										
document, each violation at issue is described as a "violation of CIP-010-2 R1. Sampling conducted during the Compliance Audit and a subsequent extent of condition analysis uncovered multiple Cyber of the procedural posture and whether it was a possible, or confirmed violation.) (in the procedural posture and used to track patches and software for numerous devices. The Entity would typically document its baselines in either its baseline tool or its patch management system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. Was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber of did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible.	yber Assets that did two devices and the t system (an alternate col. The software per Asset. The Entity ssible discrepancies.										
"violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.) In thave baselines that included all installed commercially available software as required by P1.1. The Entity did not include the software on the documented baseline for two includes that include all installed commercially available software as required by P1.1. The Entity did not include the includes the documented baseline for two includes the software on the documented baseline for two in the software on the documented baseline tool. In the software on the documented baseline tool on the software on the documented baseline too	two devices and the t system (an alternate col. The software per Asset. The Entity ssible discrepancies.										
whether it was a possible, or confirmed violation.)Entity did not sufficiently identify the software for numerous devices. The Entity would typically document its baselines in either its baseline tool or its patch management sy tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible the possible	t system (an alternate col. The software per Asset. The Entity ssible discrepancies.										
tracking system used to track patches and software items that cannot be tracked by its baseline tool). Both of these software applications could not be tracked in its baseline tool. was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber a did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possib	ool. The sector software per Asset. The Entity ssible discrepancies.										
was included in its patch management system, but the reference was not specific enough to identify the unique or incremental software version that was installed on each Cyber did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the reviewer towards a complete discovery of all possible of the process lacked sufficient detail to guide the process lacked sufficient det	per Asset. The Entity ssible discrepancies.										
did not detect the noncompliance during its vulnerability assessment because that process lacked sufficient detail to guide the reviewer towards a complete discovery of all possil	ossible discrepancies.										
	i										
The source of the noncompliance was the Entity's deficient process for developing baselines and detecting errors or emissions											
The cause of the honcompliance was the Entity's dencient process for developing baselines and detecting errors or omissions.	The cause of the honcompliance was the Entity's dencient process for developing baselines and detecting errors of offissions.										
Risk Assessment This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). For all affected Cyber Assets, with the exception of noncompliance was limited to not including sufficient detail regarding the software version as opposed to an omission. Further, the Entity had a software change process and chan specifically for the software, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an inadvertent or unapproved change.	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). For all affected Cyber Assets, with the exception of two, the noncompliance was limited to not including sufficient detail regarding the software version as opposed to an omission. Further, the Entity had a software change process and change form specifically for the software, reducing the risk of an inadvertent or unapproved change. The software was also well managed by the Entity's SMEs, reducing the risk of an unexpected change to the software. Finally, the Entity's for the software. Finally, the Entity's for the final software. Finally, the Entity's for the software was also well managed by the entity's SMEs, reducing the risk of an unexpected form. No harm is known to have occurred.										
Mitigation To mitigate this violation, the Entity:											
1) conducted an extent of condition analysis;											
2) corrected the baselines for the impacted Cyber Assets;	2) corrected the baselines for the impacted Cyber Assets;										
3) improved the process to identify any commercially available software; and	3) improved the process to identify any commercially available software; and										
4) validated the new process of identifying any commercially available or intentionally installed software.	4) validated the new process of identifying any commercially available or intentionally installed software.										
Other Factors MRO considered the scope of the honcompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applic	wise considered the scope of the noncompliance and the discovery method to be an aggravating factor in the disposition. Noncompliance that impacts a high population of applicable devices										
should be self-detected through internal controls. However, MRO determined that even though the honcompliance should not be eligible for compliance exception treatment, the	, the honcompliance										
does not warrant a mancial penalty given the minimal impact of the honcompliance upon the br3.											
MRO considered the Entity's compliance history and determined there were no relevant instances of noncompliance.	MRO considered the Entity's compliance history and determined there were no relevant instances of noncompliance.										

COVER PAGE

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	NPCC2018020347	Yes		Yes	Yes					Yes				Categories 3 – 4: 2 years Categories 1, 9: 3 years
2	NPCC2018020348	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
3	NPCC2018020350	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
4	NPCC2018020346	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
5	NPCC2018020351	Yes		Yes	Yes					Yes				Categories 3 – 4, 2 years Categories 1, 9: 3 years
6	WECC2018020039			Yes	Yes				Yes					Category 2 – 12: 2 year
7	WECC2018020282			Yes	Yes									Category 2 – 12: 2 year
8	WECC2016015862			Yes	Yes							Yes	Yes	Category 2 – 12: 2 year
9	WECC2017018174	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2017017885	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 year
11	WECC2018019006			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
12	WECC2017016941	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
13	WECC2017016928	Yes	Yes	Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
14	WECC2017016939	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
15	WECC2017016938			Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 year
16	WECC2017016940	Yes		Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
17	WECC2017016926	Yes		Yes	Yes				Yes	Yes	Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 year
18	WECC2017016929			Yes	Yes				Yes	Yes				Category 1: 3 years; Category 2 – 12: 2 year
19														
20														
21														
22														
23														
24														
26														
27														
28														
29														
30														

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redactions to the Spreadsheet Notice of Penalty in this posting and provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.
NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc			
NPCC2018020347	CIP-002-5.1a	R1.1, R1.2, R1.3	High	Lower	3/29/2017	9/4/2018	Self-			
Description of the Viola document, each violatio "violation," regardless whether it was a possib	tion (For purpose on at issue is desc of its procedural le, or confirmed	es of this cribed as a posture and violation.)	On September 5, 2018, (the entity) submitted a Self-Report stating that as a noncompliance with CIP-002-5.1a R1. The entity discovered the noncompliance through a third-party company it contracted with to entity violation started on March 29, 2017 when the entity failed to implement a process to identify its BES Cyber Systems. The violation process for identifying and rating its BES Cyber Systems. Specifically, the facility in scope the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations incorporate amendments to the NERC Reliability Standards into its compliance program.							
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Specifically may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The runs a few times a year. The entity has a Process Information (PI) system that is used for real-time performance monitoring and diagn connection were interrupted, the entity would provide data to via phone. The entity reduced the risk of its system becoming compromised by . The Low Impact system is further protected from unauthorized physical system. The unauthorized physical system is further protected from unauthorized physical system is further protected from unauthorized physical system.							
Mitigation			To mitigate this violation, the entity: contracted third-party company to create compliance program; and developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1. To prevent recurrence, the entity: implemented automated system/tasks to ensure NERC activities are tracked and completed. 							
Other Factors			 NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception to appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard recommissioning the facility. 							

thod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of							
		Mitigation							
-керогт	9/4/2018	12/12/2018							
	it had discovered	in June of 2017 it was in							
evaluate its compli	iance program	III Julie Of 2017 it was in							
evaluate its compli	iance program.								
n ended on Sentember 1, 2018 when the entity developed a									
		ie entity developed a							
entity then hired a t	third-party company	to help them evaluate							
-									
	. In particular, t	he entity did not							
eviewed, assessed,	or implemented whe	en the entity							
y, by failing to iden	tify the impact level	of its assets, the entity							
e facility in scope ha	as been classified as a	a Low Impact Asset that							
nostics. This syster	m sends information	to ; if this							
nysical access.									
treatment was not	appropriate and that	t a capition was							
auirements were c	appropriate and that	n a salicioli was mented as the entity							
quirements were t	insidered and imple	mented as the entity							

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho			
NPCC2018020348	CIP-002-5.1a	R2.1, R2.2	Lower	High	3/29/2017	9/4/2018	Self-R			
Description of the Violat document, each violatio a "violation," regardless posture and whether it v confirmed violation.)	ion (For purpose n at issue is desc of its procedural was a possible, o	s of this ribed as r	On September 3, 2018,							
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope times a year. The entity has a PI system that sends information to the could expose applicable Cyber Assets to unauthorized the entity would provide of the entity reduced the risk of its system becoming compromised by the Low Impact system is further protected from unauthorized physical access.							
Mitigation			 To mitigate this violation, the entity: 1. contracted third-party company to create compliance program; 2. developed and implement process for identifying the impact level of assets in accordance with CIP-002-5.1 Attachment 1; 3. designated a CIP Senior Manager; and 4. reviewed and obtained CIP Senior Manager Approval of the identified impact level. 							
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatme based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were co							
			based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were co the facility.							

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation								
eport	9/4/2018	12/12/2018								
e its compliance program.										
not review or have CIP Senior Manager Approval of the /ber Systems, designated a CIP Senior Manager and reviewed										
nen hired a third-r	en hired a third-party company to help them evaluate and									
or implemented iling to identify th he has been classif data to	when the entity ne impact level of its a fied as a Low Impact A via phone.	assets, the entity may fail Asset that runs a few								
ent was not appro	opriate and that a sar	iction was appropriate								
	piementeu as the ent	ity was recommissioning								

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Me			
NPCC2018020350	CIP-003-6	R1.1, R1.2	Medium	High	4/1/2017	9/4/2018	Self			
Description of the Viola document, each violatio a "violation," regardless posture and whether it confirmed violation.)	tion (For purpose on at issue is desc s of its procedura was a possible, c	s of this ribed as I or	On September 5, 2018, noncompliance with CIP-0 This violation started on A impact BES Cyber System. Specifically, the facility in s implement a compliance p The root cause of this viola	(the 103-6 R1. The entity discovere april 1, 2017 when the entity f The violation ended on Septe scope the entity discovered there w program.	entity) submitted a Self-Repor ed the noncompliance through failed to implement documente ember 4, 2018 when the entity yas a new version of the CIP sta	t stating that as a a third-party company it contracted we address of the security policies that address of	with to evaluate s Cyber Security approved its CIF ance. The entity			
Risk Assessment			The violation posed a mini review one or more docur facility in scope has been of provide data to The entity reduced the rist	Reliability Standards into its imal risk and did not pose a so nented cyber security policie classified as a Low Impact Ass via phone. k of its system becoming com	compliance program. Therefor erious or substantial risk to the s, the entity may fail to ensure set that runs a few times a year promised by	re, certain requirements were not rever reliability of the bulk power system. CIP protections are afforded and main r. The entity has a PI system that send further protected from unauthorized	Specifically, by intained, which ds information t			
Mitigation			 To mitigate this violation, the entity: 1. contracted third-party to create compliance program; 2. implemented Cyber Security Awareness training; 3. implemented Cyber Security Incident Response Plan; 4. performed tabletop exercise of Cyber Security Incident Response Plan; and 5. created a facility specific CIP-003-6 procedure. 							
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatmet based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were control to the facility.							

\$10,000

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation								
eport	9/18/2018	5/24/2019								
, it had discovered in June of 2017 it was in s compliance program.										
wareness and Cyber Security Incident Response for its low 103-6 Cyber Security – Security Management Controls policy.										
nen hired a third-p	party company to help	o them evaluate and								
or implemented v	In particular, the ent when the entity	tity did not incorporate								
build expose applie	cable Cyber Assets to s connection were int	unauthorized use. The errupted the entity would								
ent was not approonsidered and im	opriate and that a san plemented as the ent	iction was appropriate ity was recommissioning								

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			
NPCC2018020346	CIP-003-6	R2.	Lower	Severe	4/1/2017	9/4/2018	Self-Report	9/6/2018	5/24/2019			
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or			On September 5, 2018, noncompliance with CIP-00 This violation started on A	On September 5, 2018,, it had discovered in June of 2017 it was in noncompliance with CIP-003-6 R2. The entity discovered the noncompliance through a third-party company it contracted with to evaluate its compliance program.								
confirmed violation.)	impact BES Cyber System. The violation ended on September 4, 2018 when the entity implemented its approved CIP-003-6 Cyber Security – Security Management Controls policy Specifically, the facility in scope the entity discovered there was a new version of the CIP standards and that it was not in compliance. The entity did not have in place documented cyber security pl addressed the sections in CIP-003-6 Attachment 1. The entity then hired a third-party company to help them evaluate and implement a compliance program. The root cause of this violation was a lack of awareness of several NERC Reliability Standard requirement obligations The root cause of the NERC Reliability Standards into its compliance program. Therefore, certain requirements were not reviewed assessed, or implemented when the entity											
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify the impact level of its assets and create and review one or more documented cyber security policies, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use. The facility in scope has been classified as a Low Impact Asset that runs a few times a year. The entity has a PI system that sends information to row in provide data to									
Mitigation			To mitigate this violation, t 1. Contracted third-p 2. Implemented Cybe 3. Implemented Cybe 4. Performed tableto 5. Created a facility s To prevent recurrence, the 1. implemented auto	To mitigate this violation, the entity: Contracted third-party to create compliance program; Implemented Cyber Security Awareness training; Implemented Cyber Security Incident Response Plan; Performed tabletop exercise of Cyber Security Incident Response Plan; and Created a facility specific CIP-003-6 procedure. To prevent recurrence, the entity: implemented automated automated system (tacks to function as a compliance calendar to ensure NERC activities are tracked and completed. 								
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.									

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		
NPCC2018020351	CIP-003-6	R3.	Medium	Severe	4/1/2017	9/4/2018	Self-Report	9/4/2018	12/12/2018		
Description of the Viola document, each violati a "violation," regardles posture and whether it confirmed violation.)	ation (For purpose on at issue is desc ss of its procedura t was a possible, o	es of this cribed as l or	On September 5, 2018, noncompliance with CIP-00 This violation started on Ap Specifically, the facility in s t implement a compliance p The root cause of this viola	(the D3-6 R3. The entity discover pril 1, 2017 when the entity cope he entity discovered there w rogram. tion was a lack of awarenes	entity) submitted a Self-Reported the noncompliance throug failed to identify a CIP Senior f vas a new version of the CIP st s of several NERC Reliability St	rt stating that as a hard requirement obligations	, it th to evaluate its compliance pro n September 4, 2018 when the e. The entity then hired a third-	had discovered in Jun ogram. entity designated a Cl party company to hel	e of 2017 it was in P Senior Manager. p them evaluate and tity did not incorporate		
Risk Assessment			amendments to the NERC The violation posed a mini- individual responsible for e failing to implement these facility in scope has been c provide data to The entity reduced the risk	Reliability Standards into its mal risk and did not pose a s ensuring compliance. As a re controls to ensure compliar lassified as a Low Impact As via phone. t of its system becoming con	compliance program. Therefore rerious or substantial risk to the sult the entity failed to identifuce, the entity may fail to ensu set that runs a few times a year appromised by times a year . The Low Impact system is	fore, certain requirements were not revie be reliability of the bulk power system. Sp by the impact level of its assets and failed are CIP protections are afforded and main ar. The entity has a PI system that sends further protected from unauthorized phy	wed, assessed, or implemented pecifically, by failing to identify a to create and review one or mo ntained, which could expose app information to, if thi ysical access.	when the entity CIP Senior Manager 1 re documented cyber licable Cyber Assets t s connection were int	the entity didn't have an r security policies. By o unauthorized use. The rerrupted the entity would		
Mitigation			To mitigate this violation, the entity: identified and documented by name the CIP Senior Manager; contracted third-party to create compliance program; and created a facility specific CIP-003-6 procedure. To prevent recurrence, the entity: implemented automated system/tasks to function as a compliance calendar to ensure NERC activities are tracked and completed 								
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance. Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate and that a sanction was appropriate based on the lack of due diligence and overall lack of NERC compliance awareness to ensure NERC Reliability Standard requirements were considered and implemented as the entity was recommissioning the facility.								

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		
WECC2018020039	CIP-004-3a	R3	Medium	High	8/6/2015 (when electronic access	5/3/2018 (when a PRA was	Self-Report	5/3/2018	4/3/2019		
					was provisioned without a PRA)	performed)					
Description of the Violation (For purposes of this			In July 18, 2018, the entity submitted a Self-Report stating that, as a submitted submitted a Self-Report stating that, as a submitted submit								
document, each violation	on at issue is des	cribed as a									
whether it was a possible or confirmed violation.)			The entity conducted an internal audit beginning in October 2017, as part of mitigation related to two previous violations for the same Standard and Requirement and realized a gap in adherence to its procedures for ensuring that a Personnel Risk Assessment (PRA) was conducted for individuals authorized for electronic access to Critical Cyber Assets (CCAs). In January of 2018, the affected departments that utilize those access management procedures met to discuss and address the gap in adherence, with internal controls. While implementing one of the controls, the entity identified one employee who was authorized and granted electronic access on August 6, 2015 to software on a CCA used for outage coordination, without first having a completed PRA for the person								
			Because the entity did not	perform a PRA on the emp	loyee, they were not in the PRA tracki	ing database, which the entity used t	o help reconcile employ	ees with CIP electror	ic and physical access.		
			The entity did not have an days of noncompliance.	y other controls in place wi	thin its processes to identify the issue	sooner. On May 3, 2018, the entity p	performed the missing P	RA for the one emplo	oyee, for a total of 1,002		
The root cause of this violation was the entity's personnel not following documented procedures, which required processing of CIP electronic performed the PRAs, prior to the access being granted.								quests through the d	epartment that		
			After reviewing all relevan	t information, WECC deterr	nined the entity failed to conduct a PI	RA for one employee prior to granting	g electronic access to C(CAs, as required by CI	P-004-3a R3.		
Risk Assessment			This violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to conduct a PRA for one employee prior to granting electronic access to CCAs, as required by CIP-004-3a R3.								
			The entity had no internal controls implemented to detect or prevent this violation for nearly three years. Given the extent of the employee's access within the outage scheduling software, had they had malicious intent, they could have caused significant harm. However, the employee was authorized to have the electronic access and was sufficiently trained to use the software to perform their lich. Additionally, the internal control, that was implemented in place as part of the mitigation of previous violations, identified the single individual that did not have the PRA in the tracking								
			database. If there were any other individuals missing the PRA, this control would have identified it.								
Mitigation			To mitigate this violation, the entity:								
			1) completed a PRA for the	e one employee in scope;							
			2) re-circulated its PRA ver	rification procedure to appli	cable personnel; and						
			held a meeting with app	blicable personnel to discus	s and train for the procedures and pro	cesses that need to be followed for o	compliance. During this	meeting the attende	es agreed that the		
			will verify PRAs with access to an area, the will verify access by checking the name against the PRA Audit SharePoint list maintained by								
Other Factors			WECC reviewed the entity	's internal compliance prog	ram (ICP) and considered it to be a mi	tigating factor The entity identified t	his violation utilizing an	n internal control it h	ad implemented as part		
			of the mitigation of a prev	vious violation.							
WECC considered the entity's CIP-004-3a R3 compliance history in determining the disposition track. WECC considered the entity's CIP-004-3a R3 compliance history to be an aggravating the disposition track. WECC considered the entity's CIP-004-3a R3 compliance history to be an aggravating									n aggravating factor in		

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			
WECC2018020282	CIP-006-3c	R4	Medium	Severe	(when the first employee entered the PSP using a hard key)	8/30/2016 (when the ability to access the PSP utilizing a hard key was removed)	Self-Report	5/15/2017	10/4/2018			
Description of the Viola	Description of the Violation (For purposes of this		On , WI	ECC created a violation 1	record for the entity, as a				, for a violation of			
document, each violati	on at issue is des	cribed as a	CIP-006-3c R4. The entity had increased the scope of an existing violation of CIP-006-6 R1, given NERC Violation ID									
"violation," regardless	of its procedural	posture and	new violation record because the increase in scope had a start date of start date , which was before July 1, 2016, the mandatory and enforceable date of CIP Version 5.									
whether it was a possic	de of commed	violation.j		-		-						
			Specifically, on the control house Physical Security Perimeter (PSP) at a substation containing a Medium Impact BES Cyber System (MIBCS) with External Routable Connective (ERC). The door that was accessed had been designated to require the use of an alternate access key for entry to the PSP when electronic access controls failed or were out of servic Use of the alternate access key was intended to invoke the entity's procedure which required the Alarm Monitoring Station (AMS) to authenticate the person requesting access to alternate access key, thus enforcing two-factor authentication per the entity's physical security plan. However, the door's key core had not been changed out to the alternate access I core required for MIBCS with ERC, per the established entity security standards, during the entity's NERC CIP V5 implementation efforts. Additionally, on August 9, 2016, anot employee utilized an issued hard key to enter a control house PSP containing MIBCS with ERC. Similar to the issue mentioned above, the key core at this PSP door should have be switched out to comply with the entity's Alternate Access Key procedure which required two-factor authentication before access was permitted. After reviewing all relevant information, WECC determined the entity failed to appropriately implement its documented operational and procedural controls to manage physic access at all access of the violation was less than adequate internal controls. Specifically, the entity's CIP Version 5 project documentation did not incorporate a procedure to confirm PSP door lock cores were replaced to comply with the entity's physical security plan.									
			This violation began on Example 1 , when the first employee entered the PSP using a hard key, and ended on August 30, 2016, when the entity removed the ability to access the PSP through the alternate access door with the hard key, for a total of a days of noncompliance.									
Risk Assessment			WECC determined this	violation posed a minima	al risk and did not pose a serious of	r substantial risk to the reliability of	of the Bulk Power Sys	tem (BPS). In this in	nstance, the entity failed			
			to appropriately implement its documented operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week as required by CIP-006-3c R4.									
			However, as compensation, the entity had a very limited the number of individuals with access to its PSPs and were only those who have a legitimate business need and who had completed Personnel Risk Assessments (PRAs) and CIP training. At the time of the violation the employees who accessed the PSPs were authorized to be there and had valid PRAs. No harm is known to have occurred.									
Mitigation			To mitigate this violation 1) changed the energy	n, the entity: rgized access key cores to	o the alternate access key cores at th	he two PSPs doors in scope;						
			 conducted an audit on all alternate access key PSP doors containing MIBCS to ensure the core locks were appropriate. The entity identified six sites with key cores that were not set for utilization of alternate access keys. The entity mitigated by either installing the alternate access key cores or by inserting a non-key core lock and door handle to prohibit the door from being opened from the outside; and 									

	 updated its physical security plans to include a test checklist as an internal control. The checklist requires that the to and confirm that all other PSP doors have blank key cores.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor.
	WECC considered the entity's CIP-006 -3c R4 compliance history in determining the disposition track and considered two p disposition determination.
	Additional compliance history related to CIP-006-6 R4 were not relevant because the associated violations were related to f entity's visitor control program; and its personnel risk assessment program, respectively, which involved different conduct

tester attempt to use a specific key in all PSP door key cores previous violations to be an aggravating factor in the failing to maintain logs for physical access to PSPs; the et than the violations in this disposition.

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet NOC-2640

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		
WECC2016015862	CIP-006-6	R1 P1.1,1.2, 1.3, and 1.4	Medium	Severe		7/19/2017 (when all issues were remediated)	Self-Report	11/14/2017	7/26/2018		
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.)		es of this cribed as al posture ned	On the entity submitted a Self-Report stating that, as the self of the entity's CIP Version 3 to CIP Version 5 transitional audit on the entity's CIP Version 5 transitional audit on the self of the entity with an Area of Concern in accordance with guidance provided by NERC for CIP Version 5 transition audits. The entity then self-reported the noncompliance after receiving the audit report, knowing that the noncompliance was still occurring.								
	 Specifically, several issues were identified with the implementation of CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4. a. Regarding issue one (R1), the entity had a conference room located in its main building that was identified as a dual-purpose conference room that at times also functioned as a When not in use as a PSP, the entity did not ensure that all of the protective measures required in the Standards were applied. b. Regarding issue two (R1 Part 1.1), the entity's Physical Access Control Systems (PACS) were protected by a PSP; however, the entity utilized mechanical locks and keys that y not managed with operational or procedural controls defined in its physical security plan. 										
	c. Regarding issue three (R1 Part 1.2), the entity's employee identified substations with an access door in the control house basement connected to a tunnel, designated a of the PSP, that were found to have an emergency release (Safety) handle that did not require authentication for access into the PSP. The other end of the tunnel led to the or Entry by this manner was treated as an intrusion and would generate a response by security but did not require any type of authentication to gain access. The entity implements for egress from the confined areas of the tunnel because the PSP space was conclude a necessary evacuation route.							d to a tunnel, designated as part of the tunnel led to the outside. access. The entity implemented e PSP space was concluded to be			
			d. Regarding issue four (R1 Part 1.3), the entity did not ensure a minimum of two-factor authentication to a PSP access point at the primary Control Center containing High Impact BES Cyber Systems (HIBCS). The management of the hard keys was not well documented and did not follow a two-factor authentication for use and distribution.								
			e. Regarding issue 5 (R1 Part 1.4), the entity did not implement continuous monitoring of windows, glass, and hatches for intrusion detection when PSP motion sensors were disabled, per its procedure, throughout the workday if one or more persons entered the PSP at six substations containing MIBCS. The disabling of the motion sensors also disabled intrusion monitoring through windows, glass, and some hatches at those substations. Specifically, on July 21, 2016, the entity received a loss of communication alarm from a PSP at a substation containing MIBCS with ERC. The entity's AMS operators notified Dispatch at the 15- and 30-minute marks concerning the loss of communications with the site; however, Dispatch did not direct and authorize human observation per the established procedures.								
			After reviewing all relevant information, WECC Enforcement determined the entity; 1) failed to define operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access; where technically feasible; 3) failed to utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for unauthorized access through a physical access point into a PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively.								
The root cause of these violations was the lack of open and coordinated communication. Specifically, the different departments within the entity were not communicating or coll effectively during its implementation of Version 5 of the CIP Standards and Requirements.									communicating or collaborating		

	This violation began on and ended on Jul total of days of noncompliance.
Risk Assessment	WECC determined these violations posed a moderate risk and did not pose a serious and substantial risk to the reliability of operation or procedural controls to restrict physical access; 2) failed to utilize at least one physical access control to allow unescor individuals who have authorized unescorted physical access; 3) where technically feasible, failed to utilize two or more different physical access into PSPs to only those individuals who have authorized unescorted physical access; and 4) failed to monitor for PSP, as required by CIP-006-6 R1 Parts 1.1, 1.2, 1.3, and 1.4, respectively.
	However, the entity implemented good controls. All its PACS devices were within a designated PSP; the number of people with legitimate need to access the area, and they all had PRAs. The PACS servers were monitored for unauthorized access. Additional included tamper alarms, which would alert security officers if a cabinet were inappropriately accessed. The access tunnels were have set off an alarm, and the tunnels are not accessible from the outside. Authentication, logging, and monitoring of physical actunnel, which was the only way into the PSPs.
Mitigation	 To mitigate CIP-006-6 R1 Part 1.1, the entity has: 1) developed a key control program for alternate access to PACS servers; 2) changed the field site location from a designated PSP to a secure area and updated documentation; 3) provided test results after the PACS system was moved to its new secure areas; and 4) provided guidance for applicable personnel for identifying the required security controls for a PACS system that resides
	 To mitigate CIP-006-6 R1 Part 1.2, the entity has: identified all sites containing MIBCS that utilize the pull handle safety device; reviewed each site's tunnels and hatches for conformance to its physical security standards; developed plans for sites that deviated from the physical security standard to bring the tunnels and hatches into complian reviewed all hatches and service doors to tunnels that are not a PSP access point to ensure they are locked down and cannot ensure all tunnel doors into the PSP with the pull handle are monitored 24/7, and the use of the pull handle immediately tested that the alarms were working; and updated the response procedure that the AMS operators use to investigate "Forced Door" alarms. The pull handles are trained to respond to all forced door events.
	 To mitigate CIP-006-6 R1 Part 1.3, the entity has: 1) collected and inventoried all assigned keys to the primary Control Center; 2) developed and implemented a procedure for primary Control Center key control. The referenced operations bulletin wa available to employees; 3) updated the Physical Security Plan to change security responsibilities to security personnel and posted an operations be employees; 4) assigned the PSP keys for the primary Control Center to Physical Security organization and stored them within a secure key management program to the Physical Security organization; and 6) audited the updated procedure for effectiveness.
	To mitigate CIP-006-6 R1 Part 1.4, the entity has: 1) enhanced the training program and procedures between AMS and Dispatch to deploy resources for physical observati System procedure; and

1 19, 2017, when the entity remediated all the issues, for a

the BPS. In these instances, the entity, 1) failed to define orted physical access into each applicable PSP to only those ont physical access controls to collectively allow unescorted runauthorized access through a physical access point into a

n access to the PSPs was limited to those who had a ally, the cabinets which housed the PACS control panels e monitored around the clock, the use of the handle would access was captured for all individuals that entered the

within a PSP or outside of a PSP.

ance with its physical security standards; not be opened from the exterior of the tunnel space; ly generates a forced door event to the AMS;

documented on all PSP drawings, and AMS operators are

vas sent to AMS for their action, and the process was made

bulletin that describes the processes to the Control Center

key box residing in the security AMS;

tion within the 30 minutes required by its Loss of Security

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet NOC-2640

	2) implemented a script for contractors to read as part of their enhanced procedures between AMS and Dispatch.
Other Factors	WECC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor.
	WECC considered the entity's CIP-006-6 R1 compliance history and determined there were no relevant instances of noncomplia



NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc		
WECC2017018174	CIP-006-3c	R1; R1.1	Medium	Severe	1/13/2012 (when the substation became a Critical Asset)	12/9/2016 (when the relays were disconnected from the ESP)	Self-		
Description of the Viola document, each violatio "violation," regardless of whether it was a possib	tion (For purpose on at issue is desc of its procedural le, or confirmed	es of this cribed as a posture and violation.)	On August 14, 2017, the entity submitted a Self-Report stating that, as a second stating that were part of an Electronic Securit Specifically, the entity reported that on June 4, 2015, it discovered that second that were part of an Electronic Securit Security Perimeter (PSP) of a substation. The second were located in a second stating that were part of an Electronic Securit were used for Supervisory Control and Data Acquisition (SCADA) control between second stating and the other second were the entity identified the issue in 2015, it mistakenly marked the issue as remediated. On October 10, 2016, while performing a site val the second stating all relevant information, WECC Enforcement determined that the entity failed to ensure that all Cyber Assets within ar R1.1. The root cause of the violation was a less than adequate process. Specifically, the entity did not evaluate the ESP and PSP at the subst WECC determined that this violation began on January 13, 2012, when the substation became a Critical Asset for CIP Version 3, and e						
Risk Assessment			WECC determined that th within an ESP resided with The entity implemented n Standards. Additionally, th as compensation,	is violation posed a minima nin an identified PSP, as req to preventive or detective co ne entity had weak correctiv	I risk and did not pose a serious and su uired by CIP-006-3c R1.1. ontrols as this violation was not discov re controls as the violation was origina	ubstantial risk to the reliability of the vered within a timely manner and onl ally discovered in 2015, but marked a	BPS. II y beca s reso		
Mitigation			To remediate and mitigate 1) removed the 2) enhanced both of 3) updated its proce 4) updated its proce 5) created and provi	e this violation, the entity: from the its work management ticke dure to include instructions dure to address its assessm ded training for its updated	e ESP; eting systems to identify and track wor on what steps should be followed to ents for ESPs and PSPs; and processes and procedures to applicat	rk at BES sites or with BES Cyber Syste add a new ESP, including which Cyber ole personnel.	ems; r Asse		
Other Factors			WECC reviewed the entity The entity did not receive Self-Report date and the M The entity did not receive WECC considered the entity penalty determination.	's internal compliance prog mitigating credit for cooper Vitigation Plan submittal da mitigating credit for self-re ity's CIP-006-3c R1 compliar	ram (ICP) and considered it to be a ne ration. The entity did not quickly addr tes which was 403 days. porting because the Self-Report was s nce history in determining the penalty	eutral factor in the penalty determinates the violations, determine the fact submitted 362 days after the entity dist. WECC determined the entity's CIP-0	tion. s, and scove 06-3c		

hod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
-Report	6/13/2018	11/1/2018
ity Perimeter (ESP) perimeter fence l	were located outside	e the designated Physical mented PSP.
e used for protecti Ilidation assessmer	on of nt for CIP Version 5, t	Although he entity discovered that
n ESP resided with	in an identified PSP, a	as required by CIP-006-3c
tation for compliar	nce before or after it v	was energized.
ended on Decembe	er 9, 2016, when the	were disconnected
n this instance, the	e entity failed to ensu	re that Cyber Assets
ause the entity wa Ilved and was not r	s implementing a nev re-discovered until Oo	ver version of the CIP ctober of 2016. However,
ets should be incluc	led within the PSP;	
report mitigation	. This is evident by th	e duration between the
red the noncompli	ance.	
R1 compliance his	story to be an aggrava	ating factor in the

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet NOC-2631

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
WECC2017017885	CIP-005-5	R2; P2.3	Medium	Moderate	7/1/2016 (when the Standard and Requirement became enforceable)	4/4/2017 (when the entity modified the firewall access rules to the legacy device)	Self-Report	1/18/2019	TBD
Description of the Viola document, each violati a "violation," regardles posture and whether it confirmed violation.)	ation (For purpose on at issue is desc ss of its procedura was a possible, c	in the legacy device purposes of this est described as ocedural ssible, or Specifically, the entity submitted a Self-Report stating that, as a sible, or Specifically, the entity reported that while performing an internal controls assessment in February 2017, it discovered that intermediate device (ID) for Interactive Remote Access (IRA), which did not require multi-factor authentication, to remotely access Protected Cyber Assets (PCAs) within various ESPs for BES Cyber Systems (HIBCS) and Medium Impact BES Cyber Systems (MIBCS). The entity had replaced this legacy ID with a new IRA system which did require multi-factor authentication. It cypersonnel had been instructed to utilize the new IRA system and stop using the legacy ID. However, because the entity had not removed the firewall rules that allowed remote access to the various ESPs. After reviewing all relevant information, WECC Enforcement determined the entity failed to require multi-factor authentication for all IRA sessions, as required by CIP-005-5 R2 Part 2.3. The root cause of the violation was less than adequate internal controls and follow up. Specifically, the entity did not have controls in place to ensure that personnel were using the appropriate and IRA system, and that firewall rules were such that they prevented access to the legacy device. WECC determined that this violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on April 4, 2017, when the entity the firewall access rules from the source IP that allowed connection to the various ESPs. for a total of 278 days of noncompliance.						, it was in violation with onnel were using a legacy ESPs for High Impact entication. IT cybersecurity access to the various ESPs art 2.3.	
Risk Assessment			WECC determined that this authentication for all IRA so However, the entity impler lowered the likelihood of a	s violation posed a moderate essions to access HIBC mented strong internal contr malicious actor gaining acce	e risk and did not pose a serious and sub S and MIBCS, as required by CIP-005 rols. Specifically, the entity	ostantial risk to the reliability of the BP -5 R2 Part 2.3.	S. In this instance, the er	ntity failed to require	multi-factor . These controls
Mitigation			To remediated and mitigat 1) removed user acce 2) 4) developed new rul 5) validated connectiv 6) verified successful 7) implemented train	e this violation, the entity: ss to the ESPs from the unau es to improve firewall mana vity and created a process to explicit deny rule(s) for all a ing of the new processes to	uthorized ID; gement and tracking; o ensure that when changing rules, they dmin traffic destined to ESP networks a all firewall administrators.	are correct; re working; and			
Other Factors			WECC reviewed the entity' The entity did not receive r Report date and the Mitiga	s internal compliance progra nitigating credit for coopera ition Plan submittal date, wh	am (ICP) and considered it to be a neutr tion. The entity did not quickly address nich was 441 days.	al factor in the penalty determination. the violations, determine the facts, an	d report mitigation. This	is evident by the dur	ation between the Self-

The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the r
WECC considered the entity's CIP-005-5 R2 compliance history in determining the penalty. WECC determined the entity's CIP-005-5 R2 compli determination.

noncompliance.

liance history to be an aggravating factor in the penalty

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

					NOC-2033		<u> </u>		\$74,000		
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		
WECC2018019006	CIP-005-5	R1; P1.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became mandatory and enforceable on the entity)	4/3/2017 (when the reason for granting access was properly documented)	Self-Report	4/4/2018	5/11/2018		
Description of the Viola document, each violation	ation (For purpos on at issue is des	ses of this scribed as a	On January 19, 2018, the	entity submitted a Self-Rep	ort stating that, as a		it was in violation	n of CIP-005-5 R1.			
"violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)		posture and violation.)	Specifically, on April 3, 2017, while working on Transient Cyber Asset Access Control Lists (ACLs), the entity discovered that the reasons for granting access for five access rules were missing in the ACLs for selectronic Access Points (EAPs) to the Electronic Security Perimeters (ESPs) of selectronic Medium Impact BES Cyber Systems (MIBCS) at switching stations. Upon discovery, the entity added the appropriate reasons for granting access to the ACLs on the same day it was discovered.								
			After reviewing all relevant 005-5 R1, Part 1.3.	nt information, WECC deter	mined the entity failed to include the	e reason for granting access for inbou	ind and outbound acce	ss permissions, for	EAPs as required by CIP-		
			The root cause of the viol part of the entity's CIP Ve	ation was a lack of written o rsion 5 transition project pl	communication. Specifically, the task t an.	to review all ACLs and ensure the rea	son for granting access	was properly docume	ented; however, it was not		
			This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable on the entity, and ended on April 3, 2017, when the entity properly documented the reason for granting access within each ACL rule on the EAPs in scope, for a total of 276 days of noncompliance.								
Risk Assessment			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to include the reason for granting access for inbound and outbound access permissions, for two EAPs as required by CIP-005-5 R1, Part 1.3.								
Mitigation			This violation was a documentation issue rather than technical in nature. The entity implemented strong controls. Specifically, its network was implemented with "hub and spoke" technology in that another Cyber Asset was in place between the EAPs in scope and the external network, which had its ACL rules set to block traffic not permitted, with access comments for granting other permitted access. This setup increased the security posture and provided defense in depth. The EAPs in scope were also configured to block all traffic.								
			To mitigate this violation, the entity has:								
			1) added reasons to each of the ACLs on the EAPs and saved the two EAP configurations;								
			 created a Security Information and Event Management (SIEM) policy test that will run daily, verify that all ACLs have a comment, and send results weekly to applicable personnel; updated the CIP-005-5 procedure document to include peer review of ACLs and to ensure that comments are added to all ACLs when a new ACL is added, updated, or changed; and sent an email to the applicable personnel to notify them of the new peer review process. 								
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity's ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.								
			The entity received mitigating credit for admitting to the violation.								
			The entity did not receive mitigating credit for self-reporting due to the length of time between the discovery date and the Self-Report date.								
			WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it involved conduct distinct from this violation.								
			WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over \$50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, postevent root cause analysis and corrective action planning program.								

work was implemented with "hub and spoke" technology in that
permitted, with access comments for granting other permitted
all traffic.

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			
WECC2017016941	CIP-005-5	R1; P1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	7/14/2016 (when malicious communication detection was reestablished)	Self-Report	5/23/2018	8/22/2018			
Description of the Violat	ion (For purpos	es of this	On February 6, 2017, the e	ntity submitted a Self-Repor	t stating, as a second second , it was in vio	lation of CIP-005-5 R1.						
document, each violatio	n at issue is des	cribed as										
a "violation," regardless	of its procedur	al	On July 7, 2016, the entity	discovered, via an automate	ed alert from the management console,	, that there was a configuration issue w	vith Cyber Asset pa	irs (devices) config	ured in high availability			
posture and whether it v	was a possible, (or	fail-over configuration mod	le. These Cyber Assets were	classified as EAPs to the ESP protecting	g the High Impact BES Cyber Systems (H	HBCS). Upon further inve	estigation, the entity	determined that during its			
commed violation.j			transition to CIP Version 5,	a critical configuration setti	ng was missed in the Intrusion Detection	on System (IDS) module for each of the	EAPs pairs. All cor	figuration for the IDS	modules had been			
			completed as of July 1, 201	6 except for a single configu	iration setting. Because of the missing I	IDS module configuration setting, the E	APs did not have a meth	od for detecting know	vn or suspected malicious			
			communications for both in	nbound and outbound comr	nunications from July 1, 2016 to July 14	4, 2016, when the entity added the con	figuration settings.					
				information MECC data				o mana unicationa far b				
			After reviewing all relevant	Information, WECC determ	ined that the entity failed to have one of	or more methods for detecting known	or suspected malicious c	ommunications for b	orn indound and outbound			
			communications, as require	20 by CIP-005-5 KI Part 1.5.								
			The root cause of the violat	tion was less than adequate	controls for verifying configuration set	tings on the three EAP pairs during the	NERC CIP Version 3 to V	ersion 5 transition.				
				The root cause of the violation was less than adequate controls for verrying configuration settings on the time EAF pairs during the NERC CIP Version 5 to Version 5 transition.								
			This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on July 14, 2016, when malicious communication detection was									
			reestablished, for a total of	¹⁴ days of noncompliance.								
Risk Assessment			This violation posed a mode	erate risk and did not pose a	serious or substantial risk to the reliabi	ility of the BPS. In this instance, the enti	ity failed to have one or r	nore methods for det	ecting known or suspected			
			malicious communications for both inbound and outbound communications, as required by CIP-005-5 R1 Part 1.5.									
			However, the entity implemented strong controls. Specifically, the entity utilized a SIEM to detect changes in the configuration of devices and included commands to ensure raw data was analyzed and									
			The entity discovered this noncompliance as a result of investigating the alerts. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on									
			the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets.									
Mitigation			To mitigate this violation th	ne entity:								
			1) added the missing UDC module configuration to the									
			2) reseated the cable into	the sensor port.								
			3) created a SIFM policy t	est to monitor and detect fo	or changes.							
			4) provided training for th	e FAP with sensor port serv	ires.							
			5) ungraded the software	level on the affected	FAPs active/standby pairs: and							
			6) held a mitigation closure meeting with applicable personnel related to all compliance elements of CIP-005-5 R1									
Other Factors			WFCC reviewed the entity'	s internal compliance progra	am (ICP) and considered it to be a mitig	vating factor in the penalty determinati	on The entity's ICP dem	onstrates a strong cu	lture of compliance with a			
			focus on improving the reliability and security of the BPS.									
			The entity received mitigating credit for admitting to the violation.									
			The contraction of the set of the				ant data					
			i ne entity did not receive r	nitigating credit for self-rep	orting due to the length of time betwee	en the discovery date and the Self-Repo	ort date.					
			WECC determined that the	entity's compliance history	should not serve as a basis for aggrava	iting the penalty because it involved co	nduct distinct from this v	violation.				

					NOC-2635				\$74,000
NERC Violation ID	Reliability Standard	Req. N	/iolation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
WECC2017016941	CIP-005-5	R1; P1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	7/14/2016 (when malicious communication detection was reestablished)	Self-Report	5/23/2018	8/22/2018
WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade Project which is a multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over \$50M. This significant project addresses issues associated with the entity's aging and non-standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of the system and associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would be considered a typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause analysis and corrective action planning program.									

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

\$74	000
γ / 4 ,	,000

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet
NOC-2635

					NOC-2635				\$74,000			
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			
WECC2017016928	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	12/19/2018 (Mitigation Plan completion)	Self-Report	12/19/2018	TBD			
Description of the Violat	ion (For purpose	s of this	On February 3, 2017, the e	ntity submitted a Self-Report	t stating, as a				it was in violation			
document. each violatio	n at issue is desc	ribed as	of CIP-007-6 B2									
a "violation." regardless	of its procedural											
posture and whether it v	was a possible, or	r	Specifically for the entity's patch management process for tracking evaluating and installing other accurity patches pursuant to CID 007 6 D2 Dart 2.1. it utilized a configuration management and installing other accurity patches									
confirmed violation.)			Specifically, for the entity's patch management process for tracking, evaluating, and installing cyber security patches pursuant to CIP-007-6 R2 Part 2.1, it utilized a configuration management application to									
,			maintain a comprehensive software whitelist. The whitelist was intended to track all software and the associated security patch sources installed on all HIBCS and MIBCS BCAs, and the associated									
			Electronic Access Control a	nd Monitoring System (EACM	AS), Physical Access Control System (PA	CS), and Protected Cyber Assets (PCAs)). The software whitelist	was utilized as the sta	arting point to execute CIP-			
		1	007-6 R2 Part 2.1 through Part 2.4. On November 3, 2016, during the entity's efforts to true-up its software whitelist to the actual installed software on all its HIBCS and MIBCS BCAs and associated EACMS,									
			PACS, and PCAs, it was disc	overed that several software	applications on HIBCS BCA, EA	CMS associated with the HIBCS and	PCAs associated with	separate MIBCS, w	ere not originally captured			
in the software whitelist during the CIP Version 5 ir					lementation effort. Additionally, on De	cember 13, 2016, and February 2, 201	17, during continued effe	orts to true-up its sof	tware whitelist, the entity			
discovered another software application installed on HIBCS BCAs, Repeated PCAs and EACMS associated with the HIBCS, as well as HIBCS BCAs, respective						ectively, where the so	ftware and the associated					
			patch sources were missing	from the software whitelist	. None of this software was being track	ed for cyber security patches, therefor	e the patches were not t	peing evaluated, appli	ed, or had mitigation plans			
		1	created This issue affected	$d = BC\Delta_s$ in HIBCS and		PACS associated with the HIBCS a	e well as FACMS and		with the MIRCS for a total			
of Cyber Assets.												
			After reviewing all relevant	fter reviewing all relevant information, WECC determined the entity failed to identify a source or sources to track for the release of cyber security patches for applicable Cyber Assets that were updateable								
		1	and for which a patching source exists, for applicable Cyber Assets, as required by CIP-007-6 R2 Part 2.1. As a result, the entity also failed to evaluate security patches for applicability for the software									
			applications installed on those devices, as required by CIP-007-6 R2 Part 2.2° as well as failed to take action for the patches to either apply the patches or create a dated mitigation plan, or revise									
			an existing mitigation plan, as required by CIP-007-6 R2 Part 2.3.									
			The root cause of the violation was management policy guidance or expectations not being well-defined, understood, or enforced. Specifically, the entity had no project plans in place to address this									
			requirement, the scope of the tasks was unknown, and available resources were constrained. Additionally, there was a misalignment of the operations team's skill sets and resource assignment.									
			This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity and ended when the entity completed its mitigation plan on December 19, 2018, for a total of 902 days of noncompliance.									
Risk Assessment			This violation posed a mod	erate risk and did not pose a	serious or substantial risk to the reliabi	lity of the BPS. In this instance, the en	tity failed to identify a sc	ource or sources to tra	ack for the release of cyber			
			security patches for applica	able Cyber Assets that were	updateable and for which a patching so	urce exists, as required by CIP-007-6 R	2 Part 2.1. As a result, th	ne entity also failed to	evaluate security patches			
		1	for applicability for the soft	tware applications installed c	on those Cyber Assets, as required by Cl	P-007-6 R2 Part 2.2; as well as failed to	take action for applicab	le patches to either a	pply the patches, or create			
			a dated mitigation plan, or	revise an existing mitigation	plan, as required by CIP-007-6 R2 Part	2.3.						
			However, the entity had in	nplemented strong controls.	None of the affected Cyber Assets were	internet-facing. Furthermore, multip	le monitoring systems ar	nd methods were emp	ployed to log, detect, and			
			alert on the overall health	of the affected Cyber Assets,	, resulting in several layers of defenses r	protecting the Cyber Assets.						
Mitigation			To mitigate this violation, the entity:									
			1) inventoried all installed software applications utilizing its SIEM reporting tool, and added any missing installed software applications to asset management tool software;									
			2) used a whitelist to ensure that all installed software applications are added to and being tracked in the vulnerability management service where possible.									
			2) used a wintensi to ensure that an instance software applications are added to and being tracked in the vulnerability management service where possible;									
			3) inventoried all installed firmware and added to the vulnerability management service for tracking and evaluation of firmware in its environment;									
			uninstalled software ar	oplications that are no longe	r needed and removed them from the s	oftware whitelist;						

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet NOC-2635

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
WECC2017016928	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	12/19/2018 (Mitigation Plan completion)	Self-Report	12/19/2018	TBD
 5) updated the SIEM functions to ensure use of the best reporting tools available from the SIEM; 6) inspected the software whitelist entries for inclusion and exclusion errors that could cause software to be excluded from the evaluation work flow; 7) added functionality to its asset management tool to make it apparent to a user that an entry is either including or excluding software from the whitelist; 8) developed and documented a process for the evaluation of software and firmware entries in the software whitelist that are not able to be tracked by vulnerability management service; and 9) held training for subject matter experts (SMEs) responsible for evaluating software and firmware patches. 								nt service; and	
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS. The entity received mitigating credit for admitting to the violation. WECC considered the entity's CIP-007-6 R2 compliance history in determining the penalty. WECC determined the entity's CIP-007-6 R2 compliance history to be an aggravating factor in the penalty determination.						
			WECC applied mitigating cr multi-year effort that offici standardized transmission associated Operations and typical action of a similarly corrective action planning	redit for improvements that ally began in 2018 and is ex protection system that not Planning compliance. This a situated utility. The project program.	the entity was making on its system. The pected to be completed in 2023 at a tota only enhances the management and sec bove and beyond action is effectively a was not undertaken as the result of a m	ne entity has initiated a System-Wide T al cost of over \$50M. This significant pr curity of the new CIP protection system redesign and deployment of the entity nitigation plan. Rather, it was the result	ransmission Protection S roject addresses issues a devices, but also impro 's protection system wh t of the entity's systemat	Standardization and L ssociated with the er ves the overall reliabi ich is well beyond wh tic, post-event root ca	Jpgrade Project which is a htity's aging and non- lity of the system and at would be considered a huse analysis and

					NOC 2033				₽7 - ,000
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
WECC2017016939	CIP-007-6	R3; P3.1	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	5/19/2017 (when the physical ports were locked and added antivirus to the PCA)	Self-Report	4/10/2018	10/11/2018
Description of the Violat	ion (For purpose	s of this	On February 6, 2017, the e	ntity submitted a Self-Repor	t stating, as a	, it was in violation of CIP-007-6 R	3.		
a "violation," regardless posture and whether it v confirmed violation.)	of its procedural vas a possible, o	r	Specifically, the entity utiliz that ports on MIBC 1.1 methodology of leaving the BCAs, which was compl	ed physical port locking as of S BCAs without External Roust the physical ports instead of the physical ports instead on February 10, 2017.	one of the methods to deter, detect, or table Connectivity (ERC) had not been p of the logical ports open. Upon identific The entity did not physically port lock on	prevent malicious code on it CIP appli- port locked as of July 1, 2016. The empl cation of the missing port locks, the en e port each on the second remaining BCAs	cable Cyber Assets. How loyee responsible for thi ntity began the process o s because it was in the pr	vever, on January 19, s task mistakenly app of physically port lock rocess of decommissio	2017, the entity identified lied the CIP-007-6 R1, Part ing ports on form of oning those devices, which
it completed on December 13, 2016. Additionally, PCA did not have antivirus installed as required by CIP-007-6 R3 Part R3.1. After reviewing all relevant information, WECC determined the entity failed to deploy methods to deter, detect, or prevent malicious code on MIBCS BCAs without ERC an 007-6 R3 Part 3.1.							As without ERC and	PCA, as required by CIP-	
This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on May 19, 2017, when the entity physically port lock remaining BCAs in scope and added antivirus to the PCA, for a total of 322 days of noncompliance.							lly port locked the		
Risk Assessment			BCAs without ERC, as requi However, the entity implem also monitors network swit network segment, including	red by CIP-007-6 R3 Part 3.1 nented an extensive SIEM ar ch configurations to ensure g those without the anti-mal	ware software installed.	anges on HIBCS and MIBCS Cyber Asse	ts and alerts the operati This p	ons group of unautho protection is provided	for all devices on the
Mitigation			 To mitigate this violation, the second second	he entity: open ports on second of the cory escort checklist to ensur he checklist will also outline to capture cyber security co emaining second BCAs in scope; oplicable devices; C device types associated w cable personnel new process d procedure to ensure full ur om the antivirus software w	BCAs in scope; re the responsibilities of authorized esco the proper response steps to be taken i ontrols for all new cyber assets and/or with its MIBCS which were classified as B s changes; inderstanding of the documented contro ere created, scheduled, and being sent t	orts are met and to identify any potenti in the event an incident/disturbance is new device types at transmission facil CA and replaced them with devices cap Is to prevent malicious code on non-Ef to appropriate personnel for their revie	al incidents, including pl discovered; ities to prevent introduc pable of ERC; RC devices; and ew and verification that	nysical disturbances si cing any device types antivirus was installed	uch as broken tamper tape that could create a CIP or d on all applicable devices.
Other Factors			WECC reviewed the entity's focus on improving the relia	s internal compliance progra ability and security of the BP	m (ICP) and considered it to be a mitiga PS.	ting factor in the penalty determinatic	on. The entity ICP demo	nstrates a strong cult	ure of compliance with a

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadshe	et
NOC-2635	

					1100 2000				Ş7 1,000
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
WECC2017016939	CIP-007-6	R3; P3.1	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	5/19/2017 (when the physical ports were locked and added antivirus to the PCA)	Self-Report	4/10/2018	10/11/2018
			The entity received mitig WECC determined that t WECC applied mitigating multi-year effort that of standardized transmission associated Operations a typical action of a simila corrective action planning	gating credit for admitting to the the entity's compliance history g credit for improvements that ficially began in 2018 and is exp on protection system that not o nd Planning compliance. This a rly situated utility. The project ng program.	ne violation. should not serve as a basis for aggrava the entity was making on its system. T bected to be completed in 2023 at a tot only enhances the management and sec bove and beyond action is effectively a was not undertaken as the result of a n	ting the penalty because it was distinct he entity has initiated a System-Wide T cal cost of over \$50M. This significant p curity of the new CIP protection system redesign and deployment of the entity nitigation plan. Rather, it was the result	, separate, and not relev ransmission Protection S roject addresses issues a devices, but also impro 's protection system wh c of the entity's systemat	vant to this violation. Standardization and L issociated with the er ves the overall reliabi ich is well beyond wh tic, post-event root ca	Jpgrade Project which is a ntity's aging and non- ility of the system and nat would be considered a ause analysis and

									<i>Ţ.</i> .)000	
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	
WECC2017016938	CIP-007-6	R4; P4.2.2	Medium	High	11/8/2016 (when the SIEM stopped functioning correctly)	12/26/2016 (when the SIEM began logging and alerting for events)	Self-Report	5/17/2018	10/11/2018	
Description of the Viola document, each violatio a "violation," regardles posture and whether it confirmed violation.)	ation (For purpose on at issue is desc s of its procedural was a possible, o	s of this ribed as I r	On February 6, 2017, the e Specifically, on December and the associated EACM since November 8, 2016. database was not operati associated with the MIBC Furthermore, the antiviru However, during the 48-d	Specifically, on December 7, 2016 during a log review, the entity identified a potential logging issue with its SIEM, the event logging and alerting tool utilized to perform CIP-007-6 R4 for its HIBCS and MIBCS and the associated EACMS, PCAs, and PACS, as applicable, for technically capable devices. As a result, the entity worked with the SIEM vendor to determine that the SIEM database had been corrupted since November 8, 2016. Subsequently, the entity rebuilt the indexes in the database and brought the SIEM back to a normal operating state by December 26, 2016. During the 48-day span while the SIEM database was not operating correctly, Cyber Assets were not reporting to the SIEM: BCAS, EACMS devices, EACMS devices, PCAS, and PACS Cyber Asset, all associated with the HIBCS, and PCAS associated with the MIBCS. The identified Cyber Assets were still logging locally, therefore once the SIEM database was repaired, all data was able to be restored and captured for the 48-day timeframe. Furthermore, the antivirus continued to function as expected during this timeframe and could send its logs to the antivirus policy administrator console, which was capable of alerting on malicious code. However, during the 48-day span, the Cyber Assets were not able to send logs to the SIEM in order for the SIEM to generate alerts for a detected failure of Part 4.1 event logging. Because all logs were cached on the local devices, when the SIEM became operational again, all logs were forwarded on, normalized, and correlated. Any logs that would have caused an alert from the SIEM would have been						
			 Additionally, the entity reported that as a result of the issue with the SIEM, the Cyber Assets associated with its HIBCS were not included in the 15-calendar day log review during the SIEM database was not operating correctly. After reviewing all relevant information, WECC determined the entity failed to generate alerts for detected failure of Part 4.1 event logging, as required by CIP-007-6 R4 Part 4.2 Sub determined that the entity did not violate CIP-007-6 R4 Part 4.4 because logs were being reviewed at a summary level as required. The root cause of the violation was an equipment malfunction. Specifically, the entity's SIEM, which is its event logging and alerting tool, experienced a corruption of its database. This violation began on November 8, 2016, when the SIEM stopped functioning correctly, and ended on December 26, 2016, when the SIEM began logging and alerting for events, for 							
Risk Assessment			This violation posed a mod as required by CIP-007-6 F However, the entity imple Cyber Assets was mitigate which was verified at audi malicious code. Additiona date. While performing th	derate risk and did not pose a R4 Part 4.2 Sub-Part 4.2.2. emented strong controls. The ed, as the information was can it. The antivirus continued to ally, the entity implemented to be manual review of those log	serious or substantial risk to the reliabit risk of malicious code was mitigated by ched and sent to the SIEM upon re-inder function as expected during this timefr cask reminders to remind employees to gs, this noncompliance was identified.	ility of the BPS. In this instance, the enti- y the entity's implementation of antivir exing of the database. All Cyber Assets ame and could send its logs to the anti- review logs which included escalations	ity failed to generate ale us since it has the ability in question were protec virus policy administrato s up to senior manageme	rts for detected failur to log and alert. The ted within Physical Se or console, which was ent if the task is not co	e of Part 4.1 event logging, risk of loss of logs on the ecurity Perimeters (PSPs) capable of alerting on ompleted prior to the due	
Mitigation			 To mitigate this violation t corrected the SIEM da verified that the SIEM updated the CIP-007-6 created a SIEM Norma conducted a summary representative sample updated the CIP-007-6 provided training to a 	the entity: atabase corruption; database was operational ar 6 R4 procedure regarding log al Operations Dashboard that y review of logs from July 1, 2 e was used for the review; 6 R4 procedure to include all pplicable personnel on the up	nd ensured that all logs were normalized review; will exhibit the health and normal oper 2016 to the date the database indexes the new processes; and podated CIP-007-6 R4 procedures.	d and reportingno database corruptio rations of the SIEM by utilizing dynamic were rebuilt to ensure no potential Cy	on errors were displayed c insights of critical comp /ber Security Incidents v	in the console manag ponents of the SIEM; vent undetected. The	3er log; e logs were restored, and a	

					NOC-2635	1			\$74,000
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
WECC2017016938	CIP-007-6	R4; P4.2.2	Medium	High	11/8/2016 (when the SIEM stopped functioning correctly)	12/26/2016 (when the SIEM began logging and alerting for events)	Self-Report	5/17/2018	10/11/2018
Other Factors			WECC reviewed the entity' focus on improving the reli The entity received mitigat WECC considered the entit determination. WECC applied mitigating co multi-year effort that offici standardized transmission associated Operations and typical action of a similarly corrective action planning	s internal compliance progra ability and security of the Bf ing credit for admitting to th y's CIP-007-6 R4 compliance redit for improvements that ally began in 2018 and is exp protection system that not of Planning compliance. This a situated utility. The project program.	am (ICP) and considered it to be a mitiga PS. he violation. the entity was making on its system. Th bected to be completed in 2023 at a tot only enhances the management and sec bove and beyond action is effectively a was not undertaken as the result of a m	ating factor in the penalty determination CCC determined the entity's CIP-007-6 I al cost of over \$50M. This significant p curity of the new CIP protection system redesign and deployment of the entity nitigation plan. Rather, it was the result	on. The entity ICP demo R4 compliance history to roject addresses issues a n devices, but also impro r's protection system wh t of the entity's systema	nstrates a strong cult be an aggravating fa ssociated with the er ves the overall reliabi ich is well beyond wh tic, post-event root ca	ure of compliance with a ctor in the penalty Jpgrade Project which is a ntity's aging and non- ility of the system and nat would be considered a ause analysis and

					NOC-2055				\$74,000		
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		
WECC2017016940	CIP-007-6	R5; P5.5.1, P5.5.2	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	1/25/2017 (when password parameters were set for the accounts)	Self-Report	10/19/2018	TBD		
Description of the Violat document, each violatio a "violation," regardless	ion (For purpose n at issue is desc of its procedural	s of this ribed as I	On February 6, 2017, the e Specifically, on December	ntity submitted a Self-Reported a Self	rt stating, as a	it was in violation of CIP-007-6	5 R5. AIBCS BCAs at a switching	station, the entity's (Operations SMEs provided		
posture and whether it confirmed violation.)	was a possible, o	r	temporary passwords for the access system. Upon the Op and complexity in the subs (complexity), even though and complexity procedural	ne BCAs to be functionally to berations SMEs providing th tation remote access system the substation remote access ly until the scope of the pot	ested prior to their deployment into the e temporary passwords, the m for these particular BCAs did not me ss system and the BCAs could support s ential issue could be determined and co	ESP where the BCA password length SMEs identified the et the minimum password parameter uch parameters. Upon discovery, it w rrected in the substation remote ac	n and complexity would be at both the temporary pass ers as required by Part 5 S was determined that the O cess system.	automatically enforc words and the enforc ub-Part 5.5.1 (length) perations SMEs woul	ed via a substation remote cement of password length and Part 5 Sub-Part 5.5.2 d enforce password length		
			Upon further investigation parameters in place. The out of a total population o length and complexity requ	by arameters in place. The source of the substation remote access system had been corrected to meet CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.							
			After reviewing all relevant enforce password paramet	: information, WECC detern ers as required by CIP-007-6	nined the entity failed to implement a p 5 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.	rocess for password-only authentic	ation for interactive user a	ccess, either technica	illy or procedurally, and to		
			The root cause of the violat configuration prior to the e to CIP Cyber Assets. Had th	The root cause of the violation was a lack of internal controls during the entity's transition from Version 3 to Version 5. Specifically, there was insufficient run time in the entity's project plan to validate the configuration prior to the effective date of Version 5. During this time, the entity was implementing a new change management system and did not allow configuration changes, other than for emergencies, co CIP Cyber Assets. Had the entity's change management been in place at the time, it would have likely caught the misconfiguration.							
			This violation began on July 1, 2016, when the Standard and Requirement became mandatory and enforceable to the entity, and ended on January 25, 2017, when password parameters were set for the accounts to the devices in scope, for a total of 209 days of noncompliance.								
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to implement a process for password-only authentical interactive user access, either technically or procedurally, and to enforce password parameters, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2.								
			Therefore, while password set to a minimum length of	length and complexity did r five characters or more (de	not meet the CIP-007-6 R 5 Part 5.5 leng epending on the device type) and a mini	th and complexity requirements bet mum complexity of two different ch	ween July 1, 2016 and Janu aracter types during the vi	uary 25, 2017, passwo olation duration.	ord enforcement was still		
Mitigation			To mitigate this violation, the entity:								
			 updated the passwords associated with the identified Cyber Assets to meet length and complexity requirements; update the SIEM policy test to ensure it shows that the passwords for devices in scope meet the parameters of CIP-007 R5 Part 5.5; created a tool to assist in identifying CIP requirements, if any, that apply to new devices prior to approval of any final design that is planned to go through the entity's commissioning process; documented a process to capture Cyber Security controls for all new Cyber Assets prior to any commissioning of a Cyber Asset; ensured business unit procedures align to support password length and complexity for any new devices coming online; and 								

				NOC-2635							
NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
WECC2017016940	CIP-007-6	R5; P5.5.1, P5.5.2	Medium	Severe	7/1/2016 (when the Standard and Requirement became enforceable)	1/25/2017 (when password parameters were set for the accounts)	Self-Re				
			6) held a mitigation closure meeting with all mitigation SME team members, as well a representative from management, applicable Operation Completed remediation and mitigation tasks and procedures will be discussed, reviewed, and verified.								
Other Factors			WECC reviewed the entity focus on improving the re	's internal compliance progra liability and security of the Bf	am (ICP) and considered it to be a mitig PS.	ating factor in the penalty determina	ition. The				
			The entity received mitigating credit for admitting to the violation.								
			WECC determined that the entity's compliance history should not serve as a basis for aggravating the penalty because it was distinct, sepa								
			WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmis multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over \$50M. This significant project ac standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's prote typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the corrective action planning program.								

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

		\$74,000
thod of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
-Report	10/19/2018	TBD
Operations SMEs, ar	nd its	
he entity ICP demo	nstrates a strong culti	are of compliance with a

arate, and not relevant to this violation.

mission Protection Standardization and Upgrade Project which is a t addresses issues associated with the entity's aging and nonices, but also improves the overall reliability of the system and otection system which is well beyond what would be considered a ne entity's systematic, post-event root cause analysis and

				A-2 Public CI	P - Spreadsheet Notice of Penalty Consolida	ted Spreadsheet			\$74.000		
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		
WECC2017016926	CIP-010-2	R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	5/1/2017 (when baseline configurations were developed and captured)	Self-Report	3/29/2019	TBD		
Description of the Violation (For purposes of this document, each violation, "regardless of its procedural posture and whether it was a possible, or confirmed violation.) Description of CIP-010-2 R1. Specifically, on August 4, 2016, during its first performance of a bookend review of CIP-010-2 R2 Part 2.1 baseline configurations, the entity's some baseline elements might be missing from some Cyber Asset baseline configuration details. At the time, the entity believed that it may not have co a few Cyber Assets since port scanning could not be accomplished due to connectivity problems between its configuration monitoring tool and the Cyber asset in the Order asset in the cyber Asset in th							SM plete baseline config Assets. However, to re that all required and blation included Co EACMS, and EACMS, and P-010-2 R1 Part 1.1 So nents; however, the tion issues with the S when baseline configure	Es became concerned that urations captured for only examine the scope of the nd applicable CIP-010-2 R1 yber Assets (BCAs, PCAs) as being in scope of ere in violation of sub-part ub-Parts 1.1.1, 1.1.2, 1.1.4, procedure did not contain IEM. arations were developed			
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the entity failed to develop a baseline configuration individually or by a group, as required by CIP-010-2 R1 Part 1.1 Sub-Parts 1.1.1, 1.1.2, 1.1.4 and 1.1.5. However, the entity implemented strong detective controls. The entity did not implement controls to prevent this violation from occurring but did employ detective controls which identified the violation. Furthermore, multiple monitoring systems and methods were employed to log, detect, and alert on the overall health of the affected Cyber Assets, resulting in several layers of defenses protecting the Cyber Assets.								
Mitigation			 To mitigate this violation collected the number documented a procer Reliability risk; upgraded applicable provided training to for any baselines the the configuration m resides within the configuration of the second sec	n, the entity has: er and names of devices mis ess to capture cyber security e configuration monitoring to SMEs on SIEM admin, secur at are being tracked manual onitoring tool. An alternative onfiguration monitoring tool	sing baseline elements and completed b y controls for all new Cyber Assets and/o ool device profilers to compatible firmw rity, and compliance; ly (e.g. in spreadsheets), converted to O e is to track the baseline element throug l; set the as-is device state to be the curre	paseline configurations on the Cyber As or new device types at Transmission fa vare versions to ensure automated port offline Device Type in its asset managen gh configuration monitoring tool scann ent baseline;	ssets in scope; cilities to prevent introd t scan capability; nent system in order for ing if possible. The desir	ucing any device type the baseline element ed end result is that a	• that could create a CIP or t to be documented within all baseline documentation		

7) updated baseline reports to include only the required information to help SMEs more easily see if/when information is missing;

									<i> </i>	
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	
WECC2017016926	CIP-010-2	R1; P1.1.1, P1.1.2, P1.1.4, P1.1.5	Medium	High	7/1/2016 (when the Standard and Requirement became enforceable)	5/1/2017 (when baseline configurations were developed and captured)	Self-Report	3/29/2019	TBD	
			8) updated the CIP-010	D-2 R1 procedure to reflect	the changes to processes, documentation	on, and reporting that have been made	e, to include updating pr	ocedures for how to a	commission offline devices	
			that includes a proc	ess for adding manual basel	line configurations into its asset manage	ment system; and				
	9) trained applicable personnel on commissioning new CIP devices to ensure clarity on the procedure of collecting and documenting baseline data.									
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a focus on improving the reliability and security of the BPS.							
			The entity received miti	gating credit for admitting t	to the violation.					
			The entity did not receiv	ve mitigating credit for self-	reporting due to the length of time betw	reen the discovery date and the Self-Re	eport date.			
			WECC considered the er determination.	ntity's CIP-010-2 R1 complia	nce history in determining the penalty. N	WECC determined the entity's CIP-010	-2 R1 compliance history	/ to be an aggravating	factor in the penalty	
			WECC applied mitigating is a multi-year effort tha non-standardized transm and associated Operation considered a typical action analysis and corrective	g credit for improvements that officially began in 2018 ar mission protection system th ons and Planning compliance on of a similarly situated ut action planning program	hat the entity was making on its system. nd is expected to be completed in 2023 a hat not only enhances the management e. This above and beyond action is effect ility. The project was not undertaken as	The entity has initiated a System-Wid at a total cost of over \$50M. This signif and security of the new CIP protection tively a redesign and deployment of th the result of a mitigation plan. Rather,	e Transmission Protection icant project addresses in system devices, but als e entity's protection systic it was the result of the	on Standardization an ssues associated with o improves the overa tem which is well bey entity's systematic, po	d Upgrade Project which the entity's aging and Il reliability of the system ond what would be ost-event root cause	

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				
WECC2017016929	CIP-010-2	R2; P2.1	Medium	Severe	8/6/2016 (when baseline changes were not monitored)	11/11/2017 (when baseline changes commenced)	Self-Report	6/5/2018	10/11/2018				
Description of the Viol	ation (For purpose	s of this	On February 3, 2017, the e	ntity submitted a Self-Repor	t stating, as a	, it was in violation of CIP-010-2 F	32.						
document, each violat	ion at issue is desc	ribed as	Specifically, on November	1. 2016. the entity's SME	s discovered a misconfiguration within i	ts configuration monitoring tool used t	o monitor the entity's Cy	ber Asset baseline co	nfigurations. which caused				
posture and whether i	t was a possible, o	r	an EACMS associated with	the HIBCS not to have its ba	seline configuration monitored from A	ugust 6, 2016 to November 1, 2016, as	s required by CIP-010-2 I	R2 Part 2.1. During th	e entity's investigation, to				
confirmed violation.)			ensure other Cyber Assets	did not have similar issues,	it discovered additional Cyber Asse	ts where baseline configurations were	not being monitored at	least once every 35	calendar days for changes,				
			from August 6, 2016 to January 26, 2017. The Cyber Assets included BCAs, in addition to EACMS and EACMS and EACMS and EACMS associated with the HIBCS.										
			After reviewing all relevant information, WECC determined the entity failed to monitor at least once every 35 calendar days for changes to the baseline configuration, as well as document and investigate										
			detected unauthorized changes, as required by CIP-010-2 R2 Part 2.1.										
			The root cause of the violat	tion was less than adequate	procedures. Specifically, the entity had	a procedure in place to meet objectives	s of the Requirements; he	owever, the procedur	e did not contain complete				
			and accurate information t	to meet those objectives. Ac	lditionally, the entity had no procedure	in place to address the configuration a	and communication issue	es with the SEIM.					
			This violation began on Au	gust 6, 2016, when changes	to baseline configurations were not be	ing monitored, and ended on May 11, 2	2017, when monitoring o	of changes to baseline	configurations				
			commenced on the Cyber Assets in scope, for a total of 279 days of noncompliance.										
Risk Assessment			This violation posed a moderate risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to monitor at least once every 35 cale						calendar days for changes				
			to the baseline configuration	on, as well as document and	investigate detected unauthorized cha	nges, as required by CIP-010-2 R2 Part	2.1.						
			However, the entity imple	mented strong controls. Spe	cifically, the entity implemented an ass	et management system, which is used	for off-line device managed	gement to facilitate a	method to collect				
			configuration information	configuration information for Cyber Assets when it is difficult to implement technical or other controls. The information is gathered manually from the Cyber Assets in question and entered into the asset									
			management system. Additionally, the risk specific to solution of the BCAs in scope of this noncompliance was further reduced because changes to their baseline configurations could only be made through a										
Mitigation			To mitigate this violation, t	the entity:									
			1) worked with its SIEM vendor to develop and implement a solution that tracks the number of days since an asset was last monitored by the SIEM to verify successful baseline monitoring of Cyber Assets										
			for a 35-day rolling window;										
			2) implemented new con	figuration monitoring tool ru	Iles, policy tests, and reports;								
			 4) created a daily automated test to run for Cyber Assets which do not directly connect to the SIEM to ensure that manual baseline checks are performed at least once every 35 calendar days. For those 										
			Cyber Assets that exce	ed a 35-day baseline monito	ring check, a policy test will fail and the	e failure will be reflected on a daily email	ail report sent to	at least once every 5					
			5) upgraded applicable co	, onfiguration monitoring tool	device profilers to compatible firmwar	e versions to ensure automated port so	can capability;						
			6) established an interfac	e with the asset manageme	nt functionality and collected the date t	the offline device type was last checked	d and used the new rules	to calculate how lon	g since the last check;				
			7) added the offline device	ce type assets to the new con	nfiguration monitoring tool reports to r	eport on failing assets;							
			8) updated the CIP-010-2	R2 procedure to reflect the	changes to processes, documentation,	and reporting that have been made as	a result of the new repo	rting evidence; and					
			9) provided training to applicable personnel on the updated procedure.										
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity ICP demonstrates a strong culture of compliance with a										
			focus on improving the reli	iability and security of the B	PS.								
			The entity received mitigat	ting credit for admitting to th	ne violation.								
			The entity did not receive	mitigating credit for self-repo	orting due to the length of time betwee	en the discovery date and the Self-Repo	ort date.						
			WECC considered the entity's CIP-010-2 R2 compliance history in determining the penalty. WECC determined the entity's CIP-010-2 R2 compliance history to be an aggregating factor in the penalty.										
			determination.	y s cir-oto-z kz compliance	instory in determining the penalty. Wi	Let determined the entity's CIP-010-2		של מוו מצצו מעמנוווצ ומ	ctor in the pendity				

					NOC-2635	-			\$74,000
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
WECC2017016929	CIP-010-2	R2; P2.1	Medium	Severe	8/6/2016 (when baseline changes were not monitored)	11/11/2017 (when baseline changes commenced)	Self-Report	6/5/2018	10/11/2018
WECC applied mitigating credit for improvements that the entity was making on its system. The entity has initiated a System-Wide Transmission Protection Standardization and Upgrade multi-year effort that officially began in 2018 and is expected to be completed in 2023 at a total cost of over \$50M. This significant project addresses issues associated with the entity's age standardized transmission protection system that not only enhances the management and security of the new CIP protection system devices, but also improves the overall reliability of th associated Operations and Planning compliance. This above and beyond action is effectively a redesign and deployment of the entity's protection system which is well beyond what would typical action of a similarly situated utility. The project was not undertaken as the result of a mitigation plan. Rather, it was the result of the entity's systematic, post-event root cause ana									Jpgrade Project which is a Itity's aging and non- lity of the system and at would be considered a ause analysis and

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied	l redac
provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.	

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11 Category 12	CEII PROTECTION (YEARS)
1	NPCC2018020059	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
2	NPCC2018020060	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
3	NPCC2018020061	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
4	NPCC2018020063	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
5	NPCC2018020064	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
6	NPCC2018020062	Yes		Yes	Yes					Yes	Yes		Category 1: 3 years; Category 2 – 12: 2 years
7	WECC2017018752	Yes		Yes	Yes				Yes				Category 1: 3 years; Category 2 – 12: 2 year
8	WECC2018019340	Yes		Yes	Yes								Category 1: 3 years; Category 2 – 12: 2 year
9	WECC2017018489	Yes		Yes	Yes				Yes			Yes	Category 1: 3 years; Category 2 – 12: 2 year
10	WECC2017018732	Yes		Yes	Yes				Yes				
11	WECC2017017229	Yes		Yes	Yes	Yes	Yes		Yes				
12	WECC2018020044	Yes		Yes	Yes				Yes				
13	WECC2018020045	Yes		Yes	Yes	Yes	Yes		Yes				
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
25													
26													
27													
28													
29													
30													
31													
32													

ctions to the Spreadsheet Notice of Penalty in this posting and

								-					
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				
NPCC2018020059	CIP-002-5.1a	R1. (1.1., 1.2., 1.3.).	High	Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018				
Description of the Viol	ation (For nurnos	es of this	During a Compliance Audi	it conducted from	NPCC deter	mined that	(the entity) as a	was in	violation of CIP-002-5 1a				
document each violati	on at issue is des	cribed as a											
	of the number of the second		NI . (1.1., 1.2., 1.3.).										
violation, regardless	of its procedural	posture and	_						2010				
whether it was a possi	ole, or confirmed	violation.)	implemented a process to	ed on July 1, 2016 when the identify its Impact Rating c	of its Assets.	ess to assess applicable assets for	r BES Cyber Systems. The violat	ion ended on July 13,	2018 when the entity				
			Specifically, the entity's pr the entity conducted an ir why they failed to update	rocedures were based on the network of the network	ne Version 3 CIP Standards. The en d procedures were not updated, b	tity did not update its procedures ut did not see it as a major violati	s when the new version of the ion. The entity states it was full	CIP Standards went in ly aware the asset was	to effect. In July of 2018, s low impact, and that is				
			The root cause of this viol	ation was lack of accountab	pility and management oversight.								
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing to identify BES Cyber Systems that are applicable to the CIP Standards, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.										
			The entity reduced the ris	k of Cyber Assets becoming	compromised by affording physic	al and electronic protections.							
			reason for visit and the na without a company escort	All visitors to ame of their entity contact. t or expressed permission fr	the site (except visitors who will o rom the plant manager.	only be in the office area) are requ	uired to sign into the control ro Unautho	om's visitor's log. Stat prized personal are no	ing their name, date, t allowed in these areas				
			Additionally, the facility ha	as a 24 hour start-up time a e occurred as a result of this	and only runs when needed.								
Mitigation			To mitigate this violation	the entity:									
Milligation			1) Updated its Cl 2) Implemented	 To mitigate this violation, the entity: 1) Updated its CIP-002 procedure to Version 5 2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact BES Cyber Systems. 									
			To prevent recurrence, the 3) Implemented send escalatic depending on	e entity: software to create and trac on emails to overseeing pers how they are set up.	ck tasks. The system will send mul sons if the task has not been comp	Itiple automatic email reminders a bleted within a specified amount o	to the responsible person until of time. Tasks will repeat upon	the task is completed closure or with a spec	. The system will also cified frequency				

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
NPCC2018020059	CIP-002-5.1a	R1. (1.1., 1.2.,	High	Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
		1.5.].							
Other Factors			NPCC reviewed the entity'	s internal compliance progr	am (ICP) and considered it to be a nei determined there were no relevant ir	utral factor in the penalty determina istances of noncompliance.	tion.		
			Although the violation pos conduct, which included t	sed a minimal risk to the rel he deliberate failure to upd	iability of the bulk power system, NPC ate its documentation to identify the	C determined that Compliance Exce BES Cyber Systems as required by the	ption treatment was not e Standard.	appropriate based o	n the underlying

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			
NPCC2018020060	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018			
Description of the Violat document, each violatio a "violation," regardless posture and whether it v confirmed violation.)	ion (For purpose n at issue is desc of its procedural was a possible, o	s of this ribed as r	During a Compliance Audit R2. (2.1., 2.2.). This violation started on Ju July 13, 2018 when the ent Specifically, the entity's pro entity conducted an intern update documentation.	2. (2.1., 2.2.). This violation started on July 1, 2016 when the entity failed to review the identifications in requirement R1 and have its CIP Senior Manager or delegate approve the identifications. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets and had its CIP Senior Manager approve the identifications. The violation ended on July 13, 2018 when the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new version of the CIP Standards went into effect. In July of 2018, the ntity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it was fully aware the asset was low, and that is why they failed to pdate documentation.								
Risk Assessment			The violation posed a minir approve BES Cyber System use. The entity reduced the risk	mal risk and did not pose a s s that are applicable to the (of Cyber Assets becoming c	serious or substantial risk to the reliabilit CIP Standards, the entity may fail to ens	ty of the bulk power system. Specificall ure CIP protections are afforded and m electronic protections.	y, by failing to identify, in a intained, which could a solution of the soluti	eview and have its Cl expose applicable Cyb	P Senior Manager ber Assets to unauthorized			
			visit and the name of their escort or expressed permis	all visitors to tr entity contact. sion from the plant manage	ne site (except visitors who will only be i	In the office area) are required to sign i	nto the control room's v	not allowed in these	eir name, date, reason for areas without a company			
			Additionally, the facility ha	s a 24 hour start-up time an occurred as a result of this r	d only runs when needed.							
Mitigation			To mitigate this violation, t 1) Updated its CIF 2) Implemented t To prevent recurrence, the 3) Implemented s escalation ema they are set up	he entity: P-002 procedure to Version he entity's updated CIP-002 entity: oftware to create and track ils to overseeing persons if o	5 2-5.1 procedure. This resulted in an iden tasks. The system will send multiple au the task has not been completed within	ntification of one asset containing low i ntomatic email reminders to the respor a specified amount of time. Tasks will	mpact BES Cyber System nsible person until the ta repeat upon closure or v	is. sk is completed. The with a specified frequ	system will also send ency depending on how			
Northeast Power Coordina	ating Council, Inc.	(NPCC)	1		Settlement Agreement (Admit)				CIP			

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
NPCC2018020060	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors			NPCC reviewed the entity's NPCC considered the entity Although the violation pose which included the deliber	internal compliance progra ('s compliance history and d ed a minimal risk to the relia ate failure to have a CIP Seni	m (ICP) and considered it to be a neutra etermined there were no relevant insta bility of the bulk power system, NPCC d ior Manager approve the impact ratings	al factor in the penalty determination. nces of noncompliance. etermined that Compliance Exception s as required by the Standard.	treatment was not appr	opriate based on the	underlying conduct,

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				
NPCC2018020061	CIP-003-6	R3.	Medium	VSL - Severe	July 1, 2016	December 1, 2016	Audit	12/14/2018	12/18/2018				
Description of the Violat	ion (For purpo	ses of this	During a Compliance Audit conducted from , NPCC determined that as a was in violation of CIP-003-6 R3.										
document, each violatio	n at issue is de	scribed as											
a "violation," regardless	of its procedu	ral											
posture and whether it v confirmed violation.)	vas a possible,	or	This violation started on Jul	y 1, 2016 when the entity fa	ailed to identify a CIP Senior Manager by	y name. The violation ended on Decem	ber 1, 2016 when the er	itity designated a CIP	Senior Manager.				
			Specifically, the entity's pro	cedures were based on the	Version 3 CIP Standards. The entity did	not update its procedures when the n	ew version of the CIP Sta	ndards went into effo	ect.				
			The root cause of this violation	tion was lack of accountabil	ity and management oversight.								
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to ensure CIP protections are afforded and maintained, which could expose applicable Cyber Assets to unauthorized use.										
			The entity reduced the risk	ne entity reduced the risk of Cyber Assets becoming compromised by affording physical and electronic protections.									
			visit and the name of their escort or expressed permis	All visitors to the entity contact.	ie site (except visitors who will only be i r.	n the office area) are required to sign i Un	into the control room's v authorized personal are	isitor's log. Stating th not allowed in these	eir name, date, reason for areas without a company				
			Additionally, the facility has	s a 24 hour start-up time an	d only runs when needed.								
			No harm is known to have occurred as a result of this noncompliance.										
Mitigation			To mitigate this violation, the entity: 1) Designated a CIP Senior Manager										
			To prevent recurrence, the 2) Created automate	 Γο prevent recurrence, the entity: 2) Created automated tasks to maintain documentation for CIP Senior Manager designations. 									
Other Factors			NPCC reviewed the entity's	internal compliance progra	m (ICP) and considered it to be a neutra	al factor in the penalty determination.							
			NPCC considered the entity	's compliance history and d	etermined there were no relevant insta	nces of noncompliance.							

NOC -2627

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			
NPCC2018020063	CIP-002-5.1a	R1. (1.1., 1.2.,	High	VSL -Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018			
Description of the Viol document, each violat "violation," regardless whether it was a possi	ation (For purpos ion at issue is des of its procedural ble, or confirmed	es of this cribed as a posture and l violation.)	During a Compliance Audit conducted from , NPCC determined that the entity) as a was in violation of CIP-002- 5.1a R1. (1.1., 1.2., 1.3.). This noncompliance started on July 1, 2016 when the entity failed to implement a process to assess applicable assets for BES Cyber Systems. The violation ended on July 13, 2018 when the entity implemented a process to identify its Impact Rating of its Assets.									
			Specifically, the entity's put the entity conducted an ir why they failed to update The root cause of this viol	rocedures were based on the nternal audit and discovered the documentation.	ne Version 3 CIP Standards. The e d procedures were not updated, l pility and management oversight.	ntity did not update its procedures but did not see it as a major violatio	when the new version of the on. The entity states it was full	CIP Standards went in ly aware the asset was	to effect. In July of 2018, s low impact, and that is			
Risk Assessment			The violation posed a min the CIP Standards, the ent The entity reduced the ris reason for visit and the na without a company escort Additionally, the facility ha No harm is known to have	imal risk and did not pose a city may fail to ensure CIP po- k of Cyber Assets becoming All visitors to ame of their entity contact. c or expressed permission fr as a 24 hour start-up time a e occurred as a result of this	serious or substantial risk to the rotections are afforded and main compromised by affording physi the site (except visitors who will rom the plant manager.	reliability of the bulk power systen tained, which could expose applica cal and electronic protections. only be in the office area) are requi	n. Specifically, by failing to ide ble Cyber Assets to unauthori ired to sign into the control ro Unautho	ntify BES Cyber Syster zed use. om's visitor's log. Stat	ins that are applicable to ing their name, date, it allowed in these areas			
Mitigation			To mitigate this violation, 1) Updated its C 2) Implemented To prevent recurrence, th 3) Implemented send escalatic depending on	the entity: IP-002 procedure to Version the entity's updated CIP-00 e entity: software to create and trac on emails to overseeing pers how they are set up.	n 5 02-5.1 procedure. This resulted in ck tasks. The system will send mu sons if the task has not been com	n an identification of one asset cont ultiple automatic email reminders to pleted within a specified amount o	taining low impact BES Cyber S o the responsible person until of time. Tasks will repeat upon	Systems. the task is completed closure or with a spec	l. The system will also cified frequency			
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			
-------------------	-------------------------	------------------	--	--------------------------	----------------------	--------------------	------------------------	-------------------------------	--			
NPCC2018020063	CIP-002-5.1a	R1. (1.1., 1.2.,	High	VSL -Lower	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018			
		1.3.).										
Other Factors			NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.									
			Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to update its documentation to identify the BES Cyber Systems as required by the Standard.									

CIP

NOC -2627

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho			
NPCC2018020064	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit			
Description of the Violati document, each violati a "violation," regardles posture and whether it	ation (For purpose ion at issue is desc ss of its procedura t was a possible, o	es of this cribed as ll or	During a Compliance Audi (2.1., 2.2.). This violation started on Ju-	it conducted from uly 1, 2016 when the entity fa	, NPCC determ ailed to review the identifications in	requirement R1 and have its CIP	(the entity) as			
confirmed violation.)			Specifically, the entity's procedures were based on the Version 3 CIP Standards. The entity did not update its procedures when the new versi entity conducted an internal audit and discovered procedures were not updated, but did not see it as a major violation. The entity states it w update documentation.							
Risk Assessment			The violation posed a min approve BES Cyber Systen use.	imal risk and did not pose a s ns that are applicable to the (erious or substantial risk to the relia CIP Standards, the entity may fail to	ability of the bulk power system. ensure CIP protections are affor	Specifically, by fai ded and maintaine			
			The entity reduced the ris	k of Cyber Assets becoming c	ompromised by affording physical a	and electronic protections.				
			All visitors to the site (except visitors who will only be in the office area) are required to sign into the visit and the name of their entity contact.							
			escort or expressed permission from the plant manager.							
			Additionally, the facility has a 24 hour start-up time and only runs when needed.							
			No harm is known to have occurred as a result of this noncompliance.							
Mitigation			To mitigate this violation, the entity: 1) Updated its CIP-002 procedure to Version 5 2) Implemented the entity's updated CIP-002-5.1 procedure. This resulted in an identification of one asset containing low impact B							
			To prevent recurrence, th 3) Implemented escalation em they are set u	e entity: software to create and track nails to overseeing persons if t p.	tasks. The system will send multip the task has not been completed wi	e automatic email reminders to t thin a specified amount of time.	:he responsible pe Tasks will repeat ເ			
Northeast Power Coordi	nating Council. Inc	. (NPCC)	L		Settlement Agreement (Admit	:)				

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
	12/14/2018	12/18/2018						
s a , was in violation of CIP-002-5.1a R2.								
or delegate approve the identifications. The violation ended on identifications. sion of the CIP Standards went into effect. In July of 2018, the								
		that is why they failed to						
ailing to identify, r ned, which could e	eview and have its CI expose applicable Cyb	P Senior Manager er Assets to unauthorized						
e control room's v	isitor's log. Stating th	eir name, date, reason for						
ized personal are	not allowed in these a	areas without a company						
BES Cyber System	IS.							

\$0

erson until the task is completed. The system will also send upon closure or with a specified frequency depending on how NOC -2627

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
NPCC2018020064	CIP-002-5.1a	R2. (2.1., 2.2.).	Lower	VSL - Severe	July 1, 2016	July 13, 2018	Audit	12/14/2018	12/18/2018
Other Factors	ther Factors NPCC reviewed the entity's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.								
	Although the violation posed a minimal risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate based on the underlying conduct, which included the deliberate failure to have a CIP Senior Manager approve the impact ratings as required by the Standard.							underlying conduct,	

NOC -2627

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			
NPCC2018020062	CIP-003-6	R3.	Medium	VSL - Severe	July 1, 2016	December 1, 2016	Off-site Audit	12/14/2018	12/18/2018			
Description of the Violation (For purposes of this		s of this	During a Compliance Audit conducted from , NPCC determined that (the entity) as a it was in violation of CIP-003-6 R3.									
document, each violation at issue is described as												
a "violation," regardless of its procedural												
posture and whether it was a possible, or			This violation started on Ju	ly 1, 2016 when the entity f	ailed to identify a CIP Senior	Manager by name. The violation ended	on December 1, 2016 when the er	tity designated a CIP	Senior Manager.			
confirmed violation.)												
			Specifically, the entity's pro	ocedures were based on the	e Version 3 CIP Standards. The	e entity did not update its procedures w	hen the new version of the CIP Sta	indards went into effe	ect.			
			The root cause of this viola	tion was lack of accountabi	lity and management oversig	ht.						
Risk Assessment			The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, by failing designate a CIP Senior Manager, the entity may fail to									
			ensure CIP protections are	afforded and maintained, v	which could expose applicable	e Cyber Assets to unauthorized use.						
			The entity reduced the rick	of Cubor Accots becoming	compromised by offerding ph	weight and electronic protections						
			The entity reduced the risk	of Cyber Assets becoming of	compromised by altording pr	ivsical and electronic protections.						
				All visitors to t	he site (except visitors who w	vill only be in the office area) are require	d to sign into the control room's v	isitor's log. Stating th	eir name. date. reason for			
			visit and the name of their	entity contact.		, , , ,	5	5 5	, ,			
				,			Unauthorized personal are	not allowed in these	areas without a company			
			escort or expressed permis	sion from the plant manage	er.							
				24 h t + +								
			Additionally, the facility has	s a 24 nour start-up time an	id only runs when needed.							
			No harm is known to have	No harm is known to have occurred as a result of this noncompliance								
Mitigation			To mitigate this violation t	he entity:								
Intigation			1) Designated a CIP Se	enior Manager								
To prevent recurrence, the entity:												
			2) Created automate	, d tasks to maintain docume	entation for CIP Senior Manag	ger designations.						
Other Factors			NPCC reviewed the entity's	internal compliance progra	am (ICP) and considered it to	be a neutral factor in the penalty deterr	nination.					
			NPCC considered the entity's compliance history and determined there were no relevant instances of noncompliance.									

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Method of Discovery			
WECC2017018752	CIP-007-6	R5; P5.5	Medium	Severe	11/2/2016 (when password length and complexity was not enforced)	12/14/2016 (when password length and complexity were enforced)	Self-Report			
Description of the Viol document, each violat "violation," regardless whether it was a possi	ation (For purpo ion at issue is de of its procedura ble, or confirme	oses of this escribed as a al posture and d violation.)	On December 5, 2017, the entity submitted a Self-Report stating that, as a as a it was in violation with CIP-007-6 R5. Specifically, the entity reported that on November 2, 2016, while changing passwords for non-CIP devices, an employee from its passwords of two BES Cyber Assets (BCAs) using the same password requirements of the non-CIP devices which was two BES Cyber Assets (BCAs) were associated with a Medium Impact BES Cyber System (MIBCS) at the primary and backup Control Center. The entity documents the password complexity parameter requirements of CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2 for CIP devices. The employee was aut non-CIP devices. The entity discovered this noncompliance on December 9, 2016 during its quarterly access review. After reviewing all relevant information, WECC determined the entity failed to implement its documented process for password-only authentication for password parameters for length and complexity, as required by CIP-007-6 R5 Part 5.5 Sub-Parts 5.5.1 and 5.5.2. The root cause of the violation was incorrect performance due to lack of process controls around password changes. Specifically, an employee tasked w also changed the passwords on two BCAs while performing routine tasks on the non-CIP devices.							
Risk Assessment			WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the Bulk Power System (BPS). its documented process for password-only authentication for interactive user access when it did not enforce password parameters for length and complex Parts 5.5.1 and 5.5.2. The entity implemented good compensating controls.							
Mitigation			To remediate and mitigate this violation, the entity: a. changed the password length and complexity on the BCAs in scope; b. held a "Fact Finding" meeting with members of the team to discuss the CIP asset password policy and employee responsibilities related to the and c. reconfigured the BCAs in scope to no longer be CIP assets resulting in the team no longer having responsibility for CIP assets.							
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. The entity has in organized ICP. Within its ICP is a risk assessment process in which the entity analyzes risk through collaboration between several areas of the company. The entity did not receive mitigating credit for self-reporting because the Self-Report was submitted 362 days after the entity discovered the noncomplete the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the entity discovered the noncomplete the self-Report was submitted 362 days after the self-							

thod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation		
-Report	11/6/2017	9/20/2018		

) team also changed the

. The Center. The entity's policy clearly employee was authorized to change passwords for both CIP and authentication for interactive user access when it did not enforce employee tasked with changing the passwords of non-CIP devices ember 14, 2016, when the entity enforced the password length ower System (BPS). In this instance, the entity failed to implement length and complexity, as required by CIP-007-6 R5 Part 5.5 Sublities related to the importance of following document processes; sets. on. The entity has implemented a comprehensive and well

red the noncompliance.

(NOC-2625
WECC considered the entity's CIP-007-6 R5 compliance history in determining the disposition track. WECC considered the entity's CIP- determining the disposition track.

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

Last Updated 06/27/2019

P-007-6 R5 compliance history to be an aggravating factor in

(

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		
WECC2018019340	CIP-007-6	R2; P2	Medium	Severe	9/7/2017 (when cyber security patches were not tracked)	2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates)	Self-Certification	8/14/2018	9/24/2018		
Description of the Violat	tion (For purpose	s of this	On March 1, 2018, the ent	ity submitted a Self-Certifica	ation stating that as a						
document, each violation at issue is described as				, it was in violat	ion with CIP-007-6 R2.						
a "violation," regardless of its procedural											
posture and whether it was a possible, or			Specifically, the entity repo	orted that during its Self-Cer	tification review on January 16, 2018,	, the CIP Lead discovered that commerc	ial software had not bee	n evaluated for secu	rity patch applicability that		
confirmed violation.)			was installed on two Electronic Access Control and Monitoring Systems (EACMS) Cyber Assets associated with a MIBCS at its primary and backup Control Centers.								
			. The entity tracked software applicable to its								
			software had been remove question. The version of from its association to a BE software had been remove software was still residing of	ed from that list in error. The software residing Software residing S Cyber System. As that was ed from all MIBCS and association the two EACMS Cyber As	e spreadsheet listed the version of the g on the EACMS Cyber Assets was listed the only Cyber Asset listed on the spr ated Cyber Assets. He therefore anno sets.	e Contraction software residing on a sine ed on the spreadsheet incorrectly. Earli eadsheet as containing the containing so tated the entry on the spreadsheet as n	ngle Physical Access Cont ier in the year, the respo software, the Cybersecur o longer requiring assess	rol System (PACS) Cy onsible engineer remo ity Supervisor assum ment, when in fact a	ber Asset as the version in oved the PACS Cyber Asset ed that all instances of said version of the		
After reviewing all relevant information, WECC determined the entity failed to appropriately implement its patch management process to track, evaluate, and install cyber security patch Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patch 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; and for a identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by (2.1, 2.2, and 2.3, respectively.							rity patches for applicable h a patching source exists; and for applicable patches ired by CIP-007-6 R2 Parts				
			The root cause of the viola not covered in the docume	ntion was a less than adequa ented process.	ite security patch management tracki	ng process. Specifically, the task of whe	en and how to remove a	source from the secu	rity patch tracking list was		
			This violation began on Sep applicable software update	otember 7, 2017, when cybe es, for a total of 167 days of	r security patches for the two EACMS noncompliance.	should have been tracked, and ended o	n February 20, 2018, wh	en the entity tracked,	evaluated, and applied		
Risk Assessment			WECC determined that this violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the BPS. In this instance, the entity failed to appropriately implement its patch management process to track, evaluate, and install cyber security patches for applicable Cyber Assets which should include the identification of a source or sources for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists; 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; and for applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, either apply the patches, create a dated mitigation plan, or revise an existing mitigation plan, as required by CIP-007-6 R2 Parts 2.1, 2.2, and 2.3, respectively.								
			However, the entity impler	mented good compensating	controls.						
			No harm is known to have occurred.								
Mitigation			To remediate and mitigate	this violation, the entity:							
			a. evaluated the co	mmercial software updates	released since August 2, 2017;						
			b. applied applicabl	le security patches to the EA	CMS Cyber Assets in scope;						
			c. in conjunction w for the new EMS	c. in conjunction with the commissioning of the new Energy Management System (EMS), update its Security Patch Management Program, to include vendor supported monitored of security patches for the new EMS; and							
			d. provided training to stakeholders on the updates to the Security Patch Management Program.								
ReliabilityFirst Corporation	n (RFC)		Settlement Agreement (Admit)								

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
WECC2018019340	CIP-007-6	R2; P2	Medium	Severe	9/7/2017 (when cyber security patches were not tracked)	2/20/2018 (when the entity tracked, evaluated, and applied applicable software updates)	Self-Certification	8/14/2018	9/24/2018
Other Factors			WECC reviewed the entity' ICP. Within its ICP is a risk a The entity did not receive a WECC considered the entit determining the disposition	s internal compliance progra assessment process in which mitigating credit for self-repo y's CIP-007-6 R2 compliance n track.	am (ICP) and considered it to be a mitig the entity analyzes risk through collab orting because the Self-Report was sub history in determining the disposition	gating factor in the penalty determinat poration between several areas of the pmitted 362 days after the entity disco track. WECC considered the entity's C	ion. The entity has impler company. vered the noncompliance IP-007-6 R2 compliance h	nented a comprehen	sive and well organized vating factor in

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc		
WECC2017018489	CIP-003-2	R4	Medium	Severe	9/22/2010	7/12/2017	Self		
Description of the Viola document, each violatio "violation," regardless o whether it was a possib	tion (For purpose on at issue is desc of its procedural le or confirmed v	es of this cribed as a posture and violation.)	On October 18, 2017, the entity submitted a Self-Report stating, as a , it was in violation of CIP-003-2 R4. Specifically, the entity reported that on September 22, 2010, an employee from the Cyber Asset (CCA) information to the security file share. On July 11, 2017 the security group discovered the CCA information as define have been protected according to the program. With further examination of the security permissions associated with the security permissions associated with the security permissions associated with the security permissions associated all security permissions associated all security permissions associated all security permissions associated all security permissions associated with the security permissions associated all security permissions associated with the security permissions associated all security permissions associated with the security permissions associated all security permissions associated with the security permissions associated all security permissions associated with the						
Risk Assessment			did not follow the expecta This violation posed a mod classify, and protect inform The entity had implement information by someone v (MIBCS); the access simply had also implemented a d	tions outlined in the entity' derate risk and did not pose nation associated with CCA ed weak controls to preven vith malicious intent would / provided information that efense-in-depth approach t	s Information Protection Program. a serious or substantial risk to the rel s, as required by CIP-003-2 R4. t and/or detect the noncompliance. H not have provided any direct physical might be used to exploit a vulnerabili o cyber security.	liability of the bulk power system. In owever, the entity had compensating or electronic access to the High Imp ty in the entity's defenses if a malicic on to have occurred.	g cont act BE ous ac		
Mitigation			To mitigate this violation, the entity: 1) removed the CCA information from the Experimental file share; 2) created a secure Experimental file share that is designated as a BES Cyber System Information (BCSI) repository with all the approp 3) conducted BCSI Protection Program training with appropriate individuals.						
Other Factors			WECC reviewed the entity's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination CIP-003-2 R4 is significant and should have been found much sooner, had the entity had better internal controls in place; especially co and Requirement. WECC considered the entity's CIP-003 R4 compliance history in determining the penalty. WECC considered the entity's CIP-003 R4 co determination.						

thod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
-Report	11/8/2017	7/13/2018						
ne growing growing growing and notified th ned by the entity's file share, the	oup had inadvertent	ly uploaded Critical group. Program and should group noted 14						
the CCA informat	ion from the	file share.						
t information asso	ciated with CCAs, as r	required by CIP-003-2 R4.						
I who placed the CCA information on the second second file share								
stance, the entity	stance, the entity failed to implement its program to identify,							
trols in place that le ES Cyber Systems (H tor was able to per	essened the risk. Acco HBCS) or Medium Im netrate the perimete	ess to the CCA pact BES Cyber Systems r defenses. The entity						
priate controls; and	t i i i i i i i i i i i i i i i i i i i							
n. However, it is worth noting that the violation duration for onsidering the implementation of later versions of the Standard								
mpliance history to	be an aggravating fa	actor in the penalty						

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc
WECC2017018732	CIP-007-6	R5	Medium	Severe	7/1/2016	2/13/2018	Self-
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)			On December 4, 2017, the devices that did not have a Cyber Assets, catego substations did not have p enabled. The PCAs had be When CIP-007 Version 5 w lack of clarity over the inte	e entity submitted a Self-Rep methods to enforce authen prized as Protected Cyber A passwords. The PCAs contain een designated to monitor a vent into effect, these Cybe erpretation of the Requirem Cyber Assets (BCAs), for any	port stating, as a second stating , it was in tication of interactive user access. Up ssets (PCAs) associated with the Med ined software and applications writter and control the health of three r Assets were not updated to enforce nent. If the PCA lost communication to y reason,	n violation of CIP-007-6 R5. Spe oon further review conducted o ium Impact BES Cyber Systems n in-house by the entity and an at two of the substations, authentication of interactive u o the	cifically, the on July 26, 20 (MIBCS) wit administrat , and to mon ser access b
			After reviewing all relevant default passwords, per Cyl 007-6 R5 Parts 5.1, 5.4, and The root cause of the viola persons responsible for ide	in It information, WECC detern ber Asset capability; and for d 5.5 Sub-Parts 5.5.1 and 5 ation was an insufficient nu entifying and implementing	to the which the entity believes of mined the entity failed to have a meth r password-only authentication for int .5.2, respectively for three PCAs. mber of trained or experienced emplo security controls for PCAs had adequ	would have introduced risk to t nod(s) to enforce authenticatio ceractive user access, either teo oyees assigned to a task. Specif ate training and/or experience	the reliability n of interact chnically or p fically, in its t to appropri
Risk Assessment			This violation posed a mod authentication of interacti either technically or proce The entity had implement	derate risk and did not pose ive user access, where tech durally enforce password p ed weak controls to preven	e a serious or substantial risk to the rel nically feasible; change known default parameters, as required by CIP-007-6 F t and/or detect this noncompliance. F	liability of the bulk power syste passwords, per Cyber Asset ca S Parts 5.1, 5.4, and 5.5 Sub-Pa lowever, the entity had compe No harm is kno	em. In this in apability; and arts 5.5.1 an ensating cont own to have
Mitigation			To mitigate this violation, 1) adjusted the operability associated applications op devices are located 2) enabled the password f 3) changed the default pas 4) had required for default and go	the entity: of the applications on the perate as expected with the sector (); unctionality on the three PCAs; a meet with the group re eneric account passwords.	PCAs to allow for password functiona enablement of the password functior CAs to implement authentication of us and esponsible for the PCAs to review and	lity. This step will take program nality. These changes will need ser access; discuss the	nmatic and/c to be tested
Other Factors			WECC reviewed the entity WECC considered the entity determination.	's internal compliance prog	ram (ICP) and considered it to be a minimate history in determining the penalty. W	itigating factor in the penalty d /ECC considered the entity's CII	eterminatio P-007 R5 cor

hod of overy	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation							
Report	8/15/2018	TBD							
entity reported that on July 17, 2017, it discovered multiple 117, the entity verified that three hout External Routable Connectivity (ERC) at three separate or account where the password functionality had not been itor and control a and and at a third substation. ecause of potential operational and safety impacts, as well as a This delay									
v of the BFS		This delay							
ive user access, where we access, where access, where a construction to construct the second se	nere technically feasi ce password paramet ersion 5, the entity die	ble; change known ers, as required by CIP- d not ensure that the							
ately protect them	l.								
stance, the entity d for password onl d 5.5.2, respective	failed to have a meth y authentication for i ly.	od(s) to enforce nteractive user access,							
rols in place that l	essened the risk.								
occurred.									
or configuration ch and implemented	anges to ensure that I and are complicated	the devices and I by the fact that the							
ires. This discussio	on included specific t	raining related to actions							
n.									
npliance history to	be an aggravating fa	ictor in the penalty							

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc
WECC2017017229	CIP-011-2	R1	Medium	Severe	8/12/2016	8/31/2016	Self
Description of the Viola document, each violatio "violation," regardless whether it was a possib	tion (For purpose on at issue is desc of its procedural of or confirmed v	es of this cribed as a posture and <i>i</i> olation.)	On January 30, 2017, the outilized the and Monitoring System de group had utilized a updates, which included t This second server as BCSI. The for the applicable BCAs, Performing technical issues 12, 2016. However, on Automotion of all its discovered, the entity's 2016, they deleted all of t After reviewing all relevant The root cause of the viola and the entity had no pee	entity submitted a Self-Report entity submitted a Self-Report evices (EACMS) within the approach. The approach. The was fully controlled by of the applicable EACMS we third server resided CAs, and EACMS. This serve uses with the application gues 26, 2016, the entity's Windows-based HIBCS BCAs group took immediate st he backups of the serve at information, WECC determent ation was a less than adequer review process in place to	by 12/2010 ort stating, as a application as a patching tool for the N . To ensure the e first server resided for the application of the app	, it was in violation of CIP-01 Aicrosoft devices in its High Impa ne protection of the HIBCS and and contained all the pertinent and contained all the pertinent and contained all the pertinent and PCAs within the HIB ertinent information about Micro e entity's Program and most names that would be considered application and reconfigur department that the s, as well as all the EACMS device ated the server's datable eated since the reinstall from Aug securely handle its BCSI while in to a configuration error in the methy	1-2 R1. Sp ct BES Cyk and as nt informa BCS ESP. T >soft devic n, the ent ered BCSI, he HIBCS a red all mappli es, onto a base that o gust 12, 2 storage a: applic
Risk Assessment Mitigation			This violation posed a mod while in storage as require The entity had implement internal employees was re exposed did not contain u entity has a To mitigate this violation, 1) deleted its serve 2) implemented an autom	derate risk and did not pose ed by CIP-011-2 R1 Part 1.2. ed weak controls to preven estricted to those who have sernames or passwords. Wi the entity: r database files and associate ated system in order to avo	t this noncompliance. However, the e elevated privileges within the entity's thout this information, it would be dif . No h	liability of the bulk power system ntity had compensating controls s environment and all have a valic fficult for a person with malicious narm is known to have occurred.	in place the single of the second sec
Other Factors			WECC reviewed the entity	's internal compliance prog	ram (ICP) and considered it to be a mi	itigating factor in the penalty det	erminatio

hod of overy	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation							
-Report	3/1/2017	1/31/2018							
ecifically, the entity's group ber Systems (HIBCS) and associated Electronic Access Control sociated critical devices in the secure environment, the ation about Microsoft devices that required patches and the second server resided es that required patches and updates, which included tity had identified and classified the information on the first and									
but rather the server solution direct internet connectivity. In the spring of 2016, the entity's group began . The reconfiguration was completed on August cation setup process inadvertently server in its . Once the issue was contained all the									
016 to August 26, 2 s required by CIP-0 ation, BCSI was rep	2016. 11-2 R1 Part 1.2. Dicated outside the s	ecured CIP environment,							
stance, the entity failed to protect and securely handle its BCSI nat lessened the risk. The limited exposure of the BCSI to need for access to the server. The BSCI that was access any of the devices within the HIBCS or Lastly, the									
ues with manual patching.									
n.									

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Met Disc		
WECC2018020044	CIP-011-2	R1	Medium	Severe	7/1/2016	1/25/2017	Self-		
Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible or confirmed violation.)			On January 30, 2017, the e scan devices within its Phy meet CIP compliance. The . The management console cont designated as BSCI reposit	entity submitted a Self-Repo vsical Access Control System scan engine, which was par e scan engine reports the res trols the scan engine, telling On Septem sories; therefore, they did no	ort stating, as a province of the province of the baselining tool, was located of sults back to the baselining tool manage it where to scan, when to scan, what ber 28, 2016, during a review of its system of have the protective CIP controls that	it was in violation of CIP-011-2 nation related to baseline configurat gement console where they were ke to scan for, etc. The baselining tool stems, the entity discovered that bo at would normally be applied to BCS as required by CIP-004	R1. Sp ions, d ept databa oth the sl. The r 1-6 R4 F		
			After reviewing all relevan data in the baselining tool controls as required by CIF The root cause of the viola restricted and therefore p	t information, WECC deterr as BCSI resulted in it not be 2-004-6 R4 Part 4.1.3. ation was the entity's oversi rotected as BCSI.	nined the entity failed to appropriatel eing identified as a BCSI repository, wh ght of a critical device which led to the	y identify BCSI associated with its PA nich in turn caused the entity to not e misidentification of the informatio	ACS, as provide		
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this in associated with its PACS, as required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS data in the baselining tool as BCSI resulted i caused the entity to not provide the appropriate authorized electronic and physical access controls as required by CIP-004-6 R4 Part 4. The entity had implemented weak controls to prevent and/or detect this noncompliance. However, the entity had compensating cont BCSI to internal employees was restricted to those who had elevated privileges within the entity's environment and all had a valid bus logged and, as needed,						
Mitigation			To mitigate this violation, the entity: 1) identified the PACS data as BCSI; 2) added the baselining tool database and management console servers to a servers to a servers and designated them as BCSI repositories 3) deleted all baselining tool backups in the servers and rescheduled future backups to the servers ; 4) updated its process to include accurate information and expectations regarding this Standard and Requirement; 5) updated its procedure to include a specific email to be utilized for PACS-related questions; and 6) added access controls: i) authorization process to access servers ; and ii) established shared account password management; a) all account passwords were reset with system-generated strong passwords; b) account passwords <u>servers</u> ; and						
Other Factors			WECC reviewed the entity	's internal compliance prog	ram (ICP) and considered it to be a mi determined there were no relevant ir	tigating factor in the penalty determ	ninatio		

thod of covery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation						
-Report	12/19/2017	1/31/2018						
becifically, the entit device ports, service and was use	y reported that it uti es, accounts, and oth ed to run scans again . The ba	lized a baselining tool to er information used to st PACS assets aselining tool						
ase resides baselining tool dat missing controls in Part 4.1.3, and	abase and managem cluded	ent console were not						
s required by CIP-011-2 R1 Part 1.1. Failing to identify the PACS e the appropriate authorized electronic and physical access								
tained within the d	evice that should hav	ve been classified as						
nstance, the entity in it not being iden 4.1.3.	failed to appropriatel tified as a BCSI repos	y identify BCSI itory, which in turn						
trols in place that l siness need for acc	essened the risk. The ess. In addition, all	limited exposure of the was						
ies;								
in.								

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			
WECC2018020045	CIP-011-2	R1	Medium	Severe	1/12/2017	1/12/2017	Self-Report	12/19/2017	1/31/2018			
Description of the Viola	tion (For purpos	es of this	On May 1, 2017, the entity submitted a Self-Report stating, as a second									
document, each violation	on at issue is des	cribed as a	group was notified of an event related to an employee potentially sending BCSI to an external company earlier that day. The employee stated that errors began									
"violation," regardless	of its procedural	posture and	occurring with a server and since an server and serve									
whether it was a possib	le or confirmed	violation.)	resolution. provided the software that integrates the software the software that integrates the software									
			entity's configuration database to them so that they could troubleshoot the issues. The employee did not think there was an issue with sending the entity's configuration database									
			to customer Support group because: (1) the entity had a signed Mutual Nondisclosure & Confidentiality Agreement (MNDA) with (2) the information (2) was requesting was requesting									
			was typical configuration database information for a vendor to have; and (3) the employee believed that the configuration database file would not be human readable. The employee was aware of									
			the entity's	Program requirement to a	encrypt BCSI sent externally but at the	e time she did not know the informati	ion within the configura	ition database file wa	s BCSI. Inerefore, the			
			employee sent the	configuration database fi	by email. After send	Ing the email, the employee opened	the configuration datac	base file and realized	tincluded			
			ine servers were iviliaus and resided in an end and receive data for use in the entity's									
			HIBCS	and	. The purpose of	servers was to serve and re-	ceive	uata	of use in the entity s			
			After reviewing all relevar	nt information, WECC deterr	mined the entity failed to securely har	ndle its BCSI during transit, as require	d by CIP-011-2 R1 Part	1.2.				
			The root cause of the violation was an omission of steps based on assumption. Specifically, the employee that sent the data to an external vendor assumed that it was not BCSI and did not confirm									
			those assumptions prior to sending BCSI and the by email.									
Risk Assessment			This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, the entity failed to securely handle its BCSI during									
			transit, as required by CIP-011-2 R1 Part 1.2.									
			The entity had implement	ed weak controls to preven	t this noncompliance. However, the e	ntity had compensating controls in pl	lace that lessoned the ri	isk. The limited expos	ure of the BCSI to an			
			external source was restri	cted to a vendor where an l	NDA already existed and was in effect	. The BSCI that was exposed did not c	contain usernames or pa	asswords. Without th	s information, it would			
Nitization			be difficult for a person with malicious intent to access any of the devices within the HIBCS or MIBCS. No harm is known to have occurred.									
wiitigation			To mitigate this violation,	the entity:								
			1) requested and confirmed destroyed all conject of the PCSI that was emailed; and									
			2) provided additional CIP Access Training, which included training on its and the program to the employee who sent the									
Other Factors			WFCC reviewed the entity	's internal compliance prog	ram (ICP) and considered it to be a mi	itigating factor in the penalty determi	ination.					
			WECC considered the ent	ity's compliance history and	determined there were no relevant i	nstances of noncompliance.						

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redact provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	WECC2016016686	Yes		Yes	Yes					Yes				Category 1: 3 years; Category 2 – 12: 2 years
2	WECC2017017207	Yes	Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 – 12: 2 years
3	WECC2017016991			Yes	Yes							Yes		Category 2 – 12: 2 years
4	WECC2017017204			Yes	Yes						Yes			Category 2 – 12: 2 years
5	WECC2017017208	Yes	Yes	Yes	Yes					Yes	Yes			Category 1: 3 years; Category 2 - 12: 2 years
6	WECC2017017206			Yes	Yes						Yes			Category 2 – 12: 2 years
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
20														
28														
29														
30								1						
31							1	1						
32								1						
33							1	1						
34														
35														
36														

Filing Date: March 28, 2019

4	41	C	NT	- f D	14	•	11.		1
tions to	The	Nnreadsheet	INOTICE	OT PE	enaitv	1n -	This.	nosting	ana
nons to	unc	opreduoneet	1101100	0110	ciluity.	111	uns	posting	unu
		1			-			I U	

		1	1			1		1					
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				
WECC2016016686	CIP-002-5.1	R1; P1.2	High	Lower	7/1/2016 (when the Standard became mandatory and enforceable)	5/11/2017 (Mitigation Plan completion)	Self-Report	5/11/2017	6/1/2017				
Description of the Violat	ion (For purpose	s of this	On December 16, 2016, the	e entity submitted a Self-Rep	port stating that,		, it was in r	oncompliance with C	JP-002-5.1 R1.				
document, each violatio	n at issue is desc	ribed as											
a "violation," regardless posture and whether it v confirmed violation.)	of its procedural was a possible, o	r	and used to categorize the BES Assets. The first entity-approved CIP-002-5.1 BES Cyber System list was published May 12, 2015 to align with the entity's CIP Version 5 transition project. During the entity's November 2016 CIP-002-5.1 BES Cyber System review, a new preferential data source was identified and used to re-categorize the Low Impact BUK Electric System (BES) Cyber Systems (LIBCS) at a substation to Medium Impact BES Cyber Systems (MIBCS). Upon evaluation of the change, it was determined that the BES Asset information used to initially categorize the LIBCS was unclear and incomplete which resulted in the incorrect impact rating for the BES Cyber Systems at that substation. The entity had categorized the BES Cyber System at the substation as LIBCS because the initial CIP-002-5.1 analysis determined there were only lines, with connections to two other substations (weighted value of lines, with connections to four other transmission assets (weighted value of lines). Additionally, the substation had lines, with connective ty identified BES Cyber Systems was then compared and found to be consistent and did not yield any additional change to impact ratings. The newly categorized MIBCS did not have External Routable Connectivity (ERC). After reviewing all relevant information, WECC determined that the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2. Consequently, the entity did not apply the applicable CIP requirements to the MIBCS without ERC which it was required to have in place to comply with several other CIP Standards and Requirements.										
			WECC determined that this Plan.	s issue began on July 1, 2016	, when the Standard and Requirement b	became mandatory and enforceable, a	ind ended on May 11, 20	17, when the entity c	ompleted its Mitigation				
Risk Assessment			This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In this instance, the entity failed to correctly identify each of its MIBCS as defined by CIP-002-5.1 R1 sub-part 1.2. The MIBCS in scope had no ERC. The number of CIP requirements applicable to MIBCS without ERC is limited. However, where had no additional controls to detect or prevent this violation from occurring or compensate for the potential harm. Nevertheless, no harm is known to have occurred										
Mitigation			To mitigate this violation, the entity:										
			 updated its CIP-002 BES Cyber System list to include the reclassification of the BES Cyber System in scope, and obtained CIP senior management signature; updated its BES Cyber Systems Identification process to incorporate the accurate data source for CIP-002 identification; confirmed compliance or identified deficiencies with other applicable CIP Standards that require mitigation; and mitigated all CIP compliance deficiencies resulting from the identification of the MIBCS without ERC, which included patch management, baseline configuration, and cyber vulnerability assessments. 										
Other Factors			WECC reviewed internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.										

WECC considered	CIP-002-5.1 R1 compliance history in determining the disposition track. WECC considered	CIP-002-5.1 R1 comp
determination.		

pliance history to be an aggravating factor in the disposition

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Meth					
WECC2017017207	CIP-007-6	R1; P1.1	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on ()	2/28/2017 (when disabled the ports that were not needed)	Comp					
Description of the Violat	ion (For purpose	s of this	During a Compliance Audit		, WECC of	determined that						
document, each violation	n at issue is desc	ribed as		was in violation of	CIP-007-6 R1 Part 1.1							
a "violation," regardless	of its procedural	I										
posture and whether it v	vas a possible, o	or	Specifically, when wa	is preparing its baseline on a	workstation classified as a BES Cyber A	sset (BCA) associated with its Mediun	n Impact					
confirmed violation.)			were considered unneeded	were considered unneeded were slated for removal. During the audit, and provided the audit team a subscription that								
			Upon further review,	determined that the baselin	ne was correct and that the unnecessary	/ ports had been overlooked during th	ie remov					
			the primary Control Center	r's separate but associated d	ata center, and is not actively used by	to monitor or control the superv	isory con					
			WECC concluded that	failed to ensure that only the	hose logical network accessible ports th	at were determined to be needed on	a BCA w					
			The root cause of the viola	tion was due to an oversight	by the employee responsible for disab	ling the ports who did not follow	's docur					
			part of the baseline comig		ernal control to ensure employees force	wed the procedure.						
			The violation duration was 's Compliance Audit, t	The violation duration was 242 days. did not have detective controls in place that could have helped identify the issues sooner and to be a compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC applied a to an expedited settlement								
Risk Assessment			This violation posed a mini were determined to be ne	mal risk and did not pose a s eded. Such failure could rest	erious or substantial risk to the reliabili ult in a malicious actor gaining access to	ty of the bulk power system. In this in the BCA to cause harm to sca	nstance, ADA syste					
			However, the implemented access control at the Electronic Security Perimeter (ESP) to only allow approved traffic into the protected network inside the ESP. Based on the controls in place, WECC determined the likelihood of the potential harm occurring									
Mitigation			To mitigate this violation,	:								
			 disabled logical network ports determined to be unneeded on the BES Cyber Asset in scope; updated documentation to require a second be performed each time a change is made to a baseline configuration and validate it a documented a process to periodically review baseline configurations against a report of open ports to ensure only necessary logical ports trained personnel on the updated documentation and processes; and added CIP-007 as a regular agenda item for the monthly CIP Compliance meetings. 									
Other Factors			WECC reviewed state 's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.									
			WECC considered so compliance history and determined there were no relevant instances of noncompliance.									

oliance Audit 1/8/2018 1/29/2018	od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
	liance Audit	1/8/2018	1/29/2018

t BES Cyber System (MIBCS), it evaluated all ports, and those that on the BCA not reflected in the devices' baseline. val process. The BCA in scope is an engineering workstation in ntrol and data acquisition (SCADA) network.

ithin the MIBCS were enabled.

mented procedure for disabling unneeded ports that were not

lessen the violation duration. WECC believes had it not been for an aggravating factor and escalated the disposition treatment

failed to enable only logical network accessible ports that
em, which could affect s and its
vork. also implemented
ing was low.
against the baseline;
are open and that the baselines are accurate;
has a documented ICP, WECC determined that did not

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
WECC2017016991	CIP-007-6	R2; P2.1, 2.2, 2.3	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on	2/23/2017 (for Part 2.1 when included patching sources in its patch management process) 9/21/2017 (for Parts 2.2 and 2.3 when evaluated security patches and updated its mitigation plan)	Self-Report	8/2/2017	12/22/2017
Description of the Violat	ion (For nurnose	s of this	On	submitted a Self-Benort s	tating that				it was in violation of
document, each violatio a "violation," regardless posture and whether it v confirmed violation.)	n at issue is desc of its procedural vas a possible, o	ribed as	CIP-007-6 R2 Part 2.2. Specifically, reported conducted, pursuant to CIP	that, for three Cyber Assets 2-007-6 R2 Part 2.2. The dev	s classified as Bulk Electric System Cyber ices and software in scope support the p	Assets (BCAs) it did not assess security primary and backup Control Centers co	/ patches after the initial ntaining a Medium Impa	review of security pa act Bulk Electric Syste	atches on July 1, 2016 was m Cyber System (MIBCS).
After reviewing all relevant information, WECC determined a scope increase from the original Self-Report. WECC identified three additional devices classified as Protected Cyber Assett failed to maintain documentation that it had performed a patch evaluation at least once every 35 days, as required by Part 2.2. Additionally, and did not document a patch source as for one Electronic Access or Monitoring System (EACMS) and seven Physical Access Control Systems (PACS). Lastly, WECC determined that created a mitigation plan for security protected by Part 2.3.						Assets (PCA), where the set of th			
	implementation of a less than adequate security patch management program. The violation duration was 237 days for Part 2.1 and 447 days for Parts 2.2 and 2.3. did not have detective controls in place that could have helped identify the issues sooner and to less violation duration. WECC believes had it not been for did 's Compliance Audit, the violation duration would have been longer due to the lack of detective controls. Based on this, WECC appl aggravating factor and escalated the disposition treatment to an expedited settlement.						r and to lessen the , WECC applied an		
Risk AssessmentThis violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, the failed to evaluate security patches within 35 calendar days of evaluation; to document a patch source for applicable assets; to maintain documentation that it had performed patch evaluations once every 35 calendar days for its MIBCS and associated PC and PACs, pursuant to CIP-007-5 R2 Parts 2.1, 2.2 and 2.3. Such failure could potentially result in a malicious actor using known attack methods to gain control of a BES Cyber System. If control established, the malicious actor could cause reboots, freezes, or install malware in the systems. An attack on the devices in scope could cause disruption, restriction of visibility, or affect the op capabilities of systems which could lead to unintended consequences that could affect the BES.However, the likelihood of the risk occurring was significantly reduced by the preventative controlshad implemented. Specifically, the implemented protections at each Electronic Sect Perimeter (ESP) to permit only allowed traffic into and out of the ESP as well as implementing Intrusion Detection System devices to each network to detect malicious code. Three of the device question were not connected to the public internet; had no browser access or email, and were protected by CIP controls in CIP-004, CIP-005, CIP-006 and CIP-007. Infractions related to the releven devices constituted documentation failures for the Standard, however the evaluations were being conducted. In addition, to a very small municipal power company that employs has an extremely low turnover. Based on this, WECC determined that the likelihood of the potential harm occurring was low.						endar days of the last associated PCAs, EACMS em. If control was r affect the operating lectronic Security e of the devices in ted to the remaining that employs few staff and			
Mitigation To mitigate this violation, 1) updated the patch tracking w 2) installed applicable patches v 3) reviewed other supporting d 4) now maintains a list for all ap 5) added patch tracking to its bis Systems Support to continue to				ing workbook to include and thes where appropriate or n ing documents to determine all applicable devices under its bi-monthly CIP Complian ue to meet expectations over	d maintain a list of all applicable devices nitigation plans with required implemen e if additional updates were needed; the purview of the system support grou ce Meeting agenda. Regular discussions er time.	and software; Itation timeframes were developed an Ip (i.e. EACMS, PACS, and BCA switches with an appropriate level of view will	d approved by the CIP se ;); and ensure maintenance and	nior manager; I consistency across S	CADA Support and

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

	NOC-2593
Other Factors	WECC reviewed is internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner. WECC considered is compliance history and determined there were no relevant instances of noncompliance.

has a documented ICP, WECC determined that	did not

Ν	0	C-	2	5	9	3	
	-	-	_	-	-	-	

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		
WECC2017017204	CIP-004-6	R4;	Medium	Moderate	7/1/2016 (for Part 4.1 when the	12/8/2017 (when updated	Compliance Audit	12/13/2017	1/29/2018		
		P4.1,			Standard became mandatory and	documented authorization records					
		4.2			enforceable on (for access granted, and verified CIP					
						access against authorization					
					10/1/2016 (for Part 4.2 when the	records)					
					Standard became mandatory and						
Description of the Violat	ion (For number	a af thia	During a Compliance Audit								
document each violatio	n at issue is desc	rihed as	During a Compliance Audit	was in violation of	CIP-004-6 B4 Part 4 1 and Part 4 2						
a "violation." regardless	of its procedural										
posture and whether it	was a possible, o	r	Specifically, for CIP-004-6 F	4 Part 4.1. WECC determine	ed that was not able to demonstra	ate that it implemented its access mana	agement program per its	documented process	ses. documented		
confirmed violation.)	,		that it utilized an Access Re	equest Form and a CIP-004 A	Access Management Program spreadshe	eet when authorizing electronic or une	scorted physical access t	o its Medium Impact	Bulk Electric System Cyber		
			System (MIBCS) and their a	associated Cyber Assets or w	when authorizing access to designated st	torage locations. From July 1, 2016 thr	ough November 21, 201	6, granted elect	ronic and/or unescorted		
			physical access to its MIBC	S and associated Cyber Asse	ets to five employees without having cor	mpleted 's Access Request Form p	er 's Access Manag	ement and Revocatio	n Program and Procedure.		
			Relating to CIP-004-6 R4 Pa	art 4.2, states in its Acc	cess Management and Revocation Progr	ram and Procedure that quarterly revie	ws are conducted by cor	mparing Access Requ	est Forms to its CIP		
			Unescorted Physical Securi	ty Perimeter and Electronic	Security Perimeter list. However,	did not utilize the Access Request For	ms; therefore, did i	not have dated docum	nentation of the		
			verification between the lis	st of employees who have b	een authorized for access and the list of	f personnel who have access, at least o	ne each calendar quarte	r.			
			WECC concluded that	used a process other than	that which was documented and failed	to undate its desumanted presses to a	uthariza alastronia assa	a unaccorted physic	al access and/or access to		
			designated storage locations.								
			The root cause of the violation was management policy guidance or expectations were not well defined understead, or enforced. Specifically,								
			ine root cause of the violation was management policy guidance or expectations were not well-defined, understood, or enforced. Specifically, was new to CIP Standards and Requirements and its subject matter experts and compliance staff lacked understanding of required evidence and retention periods.								
			subject matter experts and	r compliance stan lacked un	derstanding of required evidence and re	etention periods.					
			The violation duration was	525 days for Part 4.1 and 43	33 days for Part 4.2. did not have	detective controls in place that could	have helped identify the	issues sooner and to	lessen the violation		
			duration. WECC believes ha	ad it not been for s 's Co	mpliance Audit, the violation duration v	vould have been longer due to the lack	of detective controls. B	ased on this, WECC a	pplied an aggravating		
			factor and escalated the disposition treatment to an expedited settlement.								
Risk Assessment			This violation posed a mini	mal risk and did not pose a	serious or substantial risk to the reliabili	ity of the BPS. In this instance, fai	led to document dated a	uthorization records	and include a business		
			need for access granting pursuant to CIP-004-6 R4 Part 4.1, and failed to verify once each calendar quarter that employees with CIP access had authorization records pursuant to CIP-004-6 R4 Part 4.2.								
			Such failure could result in unauthorized employees having electronic access, unescorted physical access and/or access to designated storage locations containing BES Cyber System information. This								
			access could intentionally o	or unintentionally lead to m	isuse of information or devices that sup	s compliance obligations; th	ereby potentially affection	ng the reliability of th	e BPS.		
			is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this WECC determined that the notential likelihood of the harm occurring was low								
				Par portor company mar en							
Mitigation			To mitigate this violation,	:							
			1) updated its Access Mana	agement and Revocation Pro	ogram and Procedure to reflect current	practices;					
			2) holds monthly meetings to discuss CIP compliance;								
			3) updated its spreadsheet	 a) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual reviews, and revocations; and 							
		4) provided training on the new Access Management and Revocation Program and Procedures.									
				1 1 1 1	(CD)				· · · · · · · · · · · · · · · · · · ·		
Other Factors			implement its ICD with affe	ernai compliance program (l	ICP) and considered it to be a neutral fac	ctor in the penalty determination. Alth	has a docum	ented ICP, WECC det	ermined that did not		
			implement its ite with effe	cuve internal controls in pla	ace to identify and mitigate this issue in						
			WECC considered 's co	ompliance history and deter	rmined there were no relevant instances	s of noncompliance.					
				- ,							

Western Electricity Coordinating Council (WECC)

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Meth	
WECC2017017208	CIP-010-2	R1; P1.1, 1.2, 1.3, and 1.4	Medium	High	7/1/2016 (when the Standard became mandatory and enforceable on	5/31/2017 (when baseline configurations were updated)	Comp	
and 1.4 Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			During a Compliance Audit was in violation of CIP-010-2 R1 Parts 1.1.4, 1.1.5, 1.2, 1.3 and 1.4. Specifically, failed to include for the provide evidence that acquisition (SCADA) for the pace state of the provide evidence that any of the require the performed when it installed for the pace state of the provide evidence that any of the require the performed when it installed for the pace state of the provide evidence that it performed CIP-010-2 R1 Parts 1.1, 1.2, 1.3, and 1.4 for the installed security patch on the PACS for the pace state of the violation was and the pace state of the pace state of the violation was and the pace state of provide that the processes were followed.					
Risk Assessment			treatment to an expedited settlement. This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, for failed accessible ports and security patches applied to assets, and failed to perform required change management activities for BES Cyber Assets and 1.4. Such failure could result in a lack of protective measures for those ports due to not knowing which ports were accessible, which could result in a lack of protective measures for those ports due to not knowing which ports were accessible.					
			devices, thereby potentia did not implement and change management this, WECC determined th	ally affecting series 's adequate internal controls to t processes would be minimi hat the likelihood of the pote	and its o ensure its documented processes for 0 ized; and to detect baseline configuratio ential harm occurring was low.	CIP-010-2 R1 were followed; to ensu n errors and change management p	re potentia rocess exc	
Mitigation			To mitigate this violation 1) updated the baseline of 2) updated its Change Co that all CIP-005, CIP-007, 3) held a meeting to discu- baseline component; 4) included baseline chan 5) will review all baseline	configurations for the device ntrol and Configuration Mar and CIP-010 security contro uss the changes to the proce nges as a standing item for di s, on an annual basis at the	is in scope; nagement Procedure to include the requ Is are met and a step to update baseline edure and offer guidance to ensure the b iscussion and reinforcement at monthly minimum, to ensure they are accurate a	ired use of a CIP-010 Change Reque configuration changes as required paselines are consistent, accurate, an CIP compliance meetings; and nd up-to-date.	st form for by CIP-010 nd updated	

Western Electricity Coordinating Council (WECC)

od of Discovery	y Mitigation Completion Date Optimized Completion of Mitigation					
liance Audit	1/22/2018	2/26/2018				
Cyber Assets; one Physical Access Control Systems (PACS) aree classified as Electronic Access Control or 2 R1 Part 1.1.4. 2016, that was not included on the device's baseline red change management activities per CIP-010-2 R1 Parts 1.2, of this software would have caused a deviation from the						

stalled security patch in the baseline configuration for one PACS

sses to ensure compliance with CIP-010-2 R1; however,

b lessen the violation duration. WECC believes had it not been blied an aggravating factor and escalated the disposition

o maintain baseline configurations to include logical network EACMS, and PACS pursuant to CIP-010-2 R1 Parts 1.1, 1.2, 1.3, build lead to cyber security vulnerabilities in those network

al incidents caused by poorly executed baseline configurations lusions. **The second second**

r the documentation of all changes, including the verification -2 R1 Part 1.3; d quickly after a well-managed change to the CIP-010 R1 part 1.1

Other Factors	WECC reviewed 's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although not implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner.
	WECC considered 's compliance history and determined there were no relevant instances of noncompliance.

\$0

NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho	
WECC2017017206	CIP-004-6	R5; P5.1	Medium	Moderate	8/24/2016 (when documented process were not followed)	12/8/2017 Mitigation Plan completion	Comp	
P5.1 Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)			During a Compliance Audit it was in violation of CIP-004-6 R5 Part 5.1. Specifically, was unable to demonstrate that it implemented its access management program per its documented processes. Access Management Program spreadsheet when revoking electronic or unescorted physical access to its Medium Impact Bulk Electric System However, was not able to provide evidence on the spreadsheet of one employee's unescorted physical access being revoked, nor did its process document. Additionally, was unable to provide evidence demonstrating that the process to remove one retiring employee's unescorted physical access document. Additionally, was unable to provide evidence demonstrating that the process to remove one retiring employee's unescorted physical access document. Additionally, was unable to provide evidence demonstrating that the process to remove one retiring employee's unescorted physical access upon a termination action. WECC reviewed an email dated August 23, 2016, which which was submitted as evidence do unescorted physical access upon a termination action. The email stated that an employee no longer worked for the City and should no longer however, the email contained no confirmation that the employee's unescorted physical access had been removed within 24 hours of the termination action.					
			After reviewing all relevant information, WECC determined a decrease in scope from the original audit finding. Subsequent to the audit, compliance of revocation of unescorted physical access for the one employee in scope. However, WECC determined that did fail to fee employee's ability for CIP access upon a termination action. The root cause of the violation was management policy guidance or expectations were not well defined, understood, or enforced. Specific demonstrate compliance and the retention periods for said evidence. The violation duration was 471 days. did not have detective controls in place that could have helped identify the issues sooner and to so an expedited settlement.					
Risk Assessment			This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, serious failed to access or the actual unescorted physical access within 24 hours after a termination action. Such failure could result in unauthorized physical or outages; thereby potentially affecting the reliability of the BPS. IDEN is a very small municipal power company that employs few staff and has an extremely low turnover. Based on this, WECC determine					
Mitigation			To mitigate this violation, 1) updated its Access Management and Revocation Program and Procedure to reflect current practices and detailed tracking of CIP access m 2) holds monthly meetings to discuss CIP compliance; 3) updated its spreadsheet to document employees that have access and to document the performance of quarterly reviews, annual review 4) provided training on the new Access Management and Revocation Program and Procedures.					
Other Factors			WECC reviewed states 's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although implement its ICP with effective internal controls in place to identify and mitigate this issue in a timely manner. WECC considered states 's compliance history and determined there were no relevant instances of noncompliance.					

		•					
od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation					
liance Audit	12/8/2017	2/8/2018					
cumented that it utilized an Access Request Form and a CIP-004 m Cyber System (MIBCS) and their associated Cyber Assets. provide any completed Access Request Forms as stated in							
ccess was initiated upon a termination action and the removals emonstrating the removal of an employee's ability for er have access to the primary and backup Control Centers; rmination action, nor was able to provide system logs to							
was able to provide WECC evidence that demonstrated low its documented processes for initiating removal of an							
lly, staff lac	lly, staff lacked the understanding of required evidence to						
lessen the violation an aggravating fa	lessen the violation duration. WECC believes had it not been for an aggravating factor and escalated the disposition treatment						
rovide evidence t access to BES Cyl	o demonstrate the re ber Systems with the	emoval of the ability for intent to cause damage					
that likelihood of the potential harm occurring was low.							
anagement;							
s, and revocations; and							
has a docume	ented ICP, WECC dete	ermined that did not					

COVER PAGE

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. NERC has applied redact provided the justifications that are particular to each noncompliance in the table below. For additional information on the CEII redaction justification, please see this document.

Count	Violation ID	Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8	Category 9	Category 10	Category 11	Category 12	CEII PROTECTION (YEARS)
1	FRCC2018019002			Yes	Yes								Yes	Category 2 – 12: 2 years
2	FRCC2018019016	Yes		Yes	Yes									Category 1: 3 years; Category 2 – 12: 2 years
3	SPP2017018137			Yes	Yes				Yes	Yes	Yes		Yes	Category 2 – 12: 2 year
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27														
28														
29														
30														
31														
32														
33														
34														
35														
36														
37														

Filing Date: February 28, 2019

tions to the	Spreadcheet	Notice of	Denalty in	thic f	ilinα (and
tions to the	spicausneet	NOLICE OI	I Chany III	uns 1	imig (anu

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			
FRCC2018019002	CIP-007-6	R2; P2.2	Medium	Severe	3/23/2017 (the day after the previous mitigation plan was completed)	3/5/2018 (when patches were evaluated and completed)	Spot Check	3/31/2018	8/10/2018			
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.)			Imitigation pian was completed) Completed) During a Spot Check conducted from January 15, 2018 through January 19, 2018, FRCC determined that the Entity, noncompliance with CIP-007-6 R2 (Part 2.2). , was in This noncompliance started on March 23, 2017, when the Entity failed to evaluate its security patches for applicability at least once every 35 calendar days on 12 out of 29 (41.4%) Cyber Assets (CA). The noncompliance ended March 5, 2018 when patches were evaluated and completed. The missed patches were for four (4) Energy Management System (EMS) servers, five (5) operator workstations within the EMS network, one (1) PACS server, and two (2) Programmable Local Access Control Panels. Although every patch was not critical, there were critical patches that missed the 35-day installation window. These missed patches could have prolonged the presence of software vulnerabilities, which, if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets. Although the patches in question did not meet the 35-day requirement, they were being installed on a quarterly basis. The entity did perform a vulnerability review and determined that during the time when the available security patches were not evaluated and applied as required, there were no known instances of unauthorized access or breaches to the entity's BES Cyber Systems and their associated EACMS, PACS, and PCAs. Specifically, the Entity CAs were being monitored by three external vendors. For all nine (9) of the CAs managed by External Vendor #2 and three (3) out of five (5) CAs managed by External Vendor #3, 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									
Risk Assessment			This noncompliance 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 execute their patch management process could have prolonged the presence of software vulnerabilities, which if exploited, could grant access to unauthorized personnel or misuse of Cyber Assets impacting the reliability of the BPS. The risk was reduced because all the devices were protected by a Physical Security Perimeter and all the Cyber Assets were within the Electronic Security Perimeter. In addition, Vendor #3 was completing the assessments quarterly instead of every 35 days. No harm is known to have occurred.									
Mitigation			To mitigate this violation, the Entity: 1) evaluated and applied all security patches; 2) designated a single vendor (Vendor #1) to monitor for all newly released security patches 3) verified with Vendor #2 their responsibility to apply security patches on monthly basis; 4) developed internal control to ensure evaluation and application of Vendor #2 security patches; 5) developed situational awareness internal control to ensure SME applies security patches, including: - set-up an email from HelpDesk to Vendor #1 SME as a reminder to coordinate patching that needs to be completed for all vendors - set-up an email from HelpDesk informing the Entity SME that patching due date is approaching; and 6) trained all applicable personnel on new processes and/or procedures.									
Other Factors			FRCC determined the Enti FRCC reviewed the Entity'	ty's internal compliance prog	gram (ICP) and positive cooperation as r	nitigating factors when determining th of noncompliance, which is considered	e penalty. to be aggravating. The p	revious extent of cor	ndition and gap			

A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

NOC-2607
assessment of the second secon

		-									
NERC Violation ID	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Violation Start Date	Violation End Date	Metho				
FRCC2018019016	CIP-007-6	R5: P5.6; 5.7	Medium	Severe	7/1/2016 (when the Entity failed to enforce password changes and limit unsuccessful authentication attempts or generate alerts)	1/24/2018 (when the Entity corrected the patching issues, updated the procedures to prevent reoccurrence, and trained appropriate personnel)	Spot C				
Description of the Viola	tion (For purpose	es of this	During a Spot Check cond	ucted from January 15, 2018	through January 19, 2018, ERCC determ	nined that the Entity					
document, each violation a "violation," regardles	on at issue is designed s of its procedura	cribed as	noncompliance with CIP-C	007-6 R5 (Parts 5.6 & 5.7).							
confirmed violation.)	was a possible,	or	generate alerts, and ender required alerting.	ed when the Standard becam ed on January 24, 2018 when	e mandatory and enforceable on July 1, the Entity updated their processes to re	, 2016, when the Entity failed to ent equire the changing of passwords an	orce passw d limited u				
			Specifically, for Part 5.6, t 007-6 R5, Part 5.6.	he Entity failed to enforce pa	ssword changes or an obligation to cha	nge the password at least once ever	y 15 calenc				
			For Part 5.7, the Entity fai (3) firewalls and four (4) s	led to implement controls to witches as required by CIP-00	limit the number of unsuccessful authe 07-6 R5, Part 5.7.	ntication attempts or generate aler	ts after a th				
			The root cause was an absence of internal controls related to password changes on shared accounts.								
Risk Assessment			This noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system.								
			Specifically, the Entity's fa	ailure to change the password	ls by the required timeframe could expo	ose the passwords to malicious indiv	iduals allov				
			This risk was increased be lockout policy or alerting reliability concerns for the	ecause some of the Cyber Ass after a certain number of fail e Entity.	ets at issue were designed to provide pe ed authentication attempts, which serve	erimeter protection to other BES Cy es to prevent unauthorized access t	ber Assets. hrough an o				
			From July 1, 2016 to June	1, 2018 there was no known	unauthorized access or breaches to any	y of the Entity's Cyber Assets.					
			No harm is known to have	e occurred.							
Mitigation			To mitigate this violation, P5.6: 1) scheduled the process 2) set up Help Desk ticket 3) reviewed all shared acc 4) changed all shared acc 5) configured to 6) generated an annual re	the Entity: of changing the passwords fo ing system that will issue auto counts to ensure that all acco ount passwords; monitor all shared accounts a eport that identifies shared acc	r shared accounts to take place each ye o-generated tickets the first month of e unts are justified and still needed; and track when passwords have been ch counts where the passwords have not l	ear during the first quarter to ensure ach year with the list of shared acco nanged; and been changed in the last 365 days.	they are counts in the				
			 P5.7: 1) updated SIEM to analyze 2) tested and verified logs 3) created rules and report 4) trained Entity personne 	ze the logs from the firewalls s for all applicable Cyber Asse rting in SIEM to produce alert el on newly instituted interna	and switches; ts in SIEM; is based on the threshold of 5 unsucces I controls for the requirement.	sful attempts occurring; and					

Florida Reliability Coordinating Council, Inc. (FRCC)

Settlement Agreement (Neither Admits nor Denies)

od of Discovery	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation
Check	6/1/2018	8/10/2018
vord changes, and	d limit unsuccessful a	, was in , was in uthentication attempts or

vord changes, and limit unsuccessful authentication attempts or unsuccessful authentication attempts as well as established

dar months for all eight (8) shared accounts as required by CIP-

hreshold of unsuccessful authentication attempts on the three

wing unauthorized access to Cyber Assets.

. Additionally, the Entity's failure to configure an account online guessing or brute force attack, could have caused

changed within the required timeframe; e body of the ticket that need to have their passwords changed; A-2 Public CIP - Spreadsheet Notice of Penalty Consolidated Spreadsheet

NOC-2607

Other Factors	FRCC determined the Entity's internal compliance program (ICP) and positive cooperation as mitigating factors when determining the penalty
	FRCC reviewed the Entity's compliance history and determined there were no relevant instances of noncompliance.

v.

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			
SPP2017018137	CIP-008-3	R1	Lower	High	3/17/2016 (fifteen months had transitioned to CIP Version 5] after successful completion of the last test)	9/26/2017 (test was successfully completed)	Self-Report	8/22/2018	1/11/2019			
Description of the Viola	tion (For purpos	es of this	On August 10, 2017,	submitted a Self-Report, st	ating that, as a			, it was in noncc	ompliance with CIP-008-3			
document, each violatio	on at issue is des	cribed as a	R1. stated that it fail	ed to perform an adequate	test of its Cyber Security Incident resp	onse plan between December 17, 20	14 and September 26, 7	2017. reports that	at it did perform a test on			
"violation," regardless of	of its procedural	posture and	March 28, 2017, but that	test did not meet sta	ndards; specifically the test was more	general than expected and did r	not include specific step	s for implementing a	response to a Cyber			
whether it was a possib	le, or confirmed	violation.)	Security Incident to the degree that expected. states that it detected this noncompliance after a new CIP Senior Manager was designated and the CIP Senior Manager conducted a full review of compliance activities.									
			The noncompliance was caused by inadequate internal controls to provide oversight regarding the completion of this task.									
Risk Assessment			The noncompliance posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. conducted a test that did not meet all the requirements of its program (albeit 11 days late), thus the risk of the noncompliance was reduced because the noncompliance was essentially for conducting an incomplete test, as opposed to not conducting any type of testing. Additionally, the subsequent testing of the Cyber Security Incident plan was successful. Finally, employees are trained under CIP-004-6 R2, which includes response and recovery to Cyber Security Incidents. No harm is known to have occurred.									
Mitigation			To mitigate this noncompliance,									
			1) performed the required test;									
			2) reviewed and revised the Cyber Security Incident response plan to better align with its standards for level of detail; and									
			3) scheduled the next required execution of the Cyber Security Incident response plan to occur within 11 months of the last test.									
Other Factors			MRO reviewed internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination.									
			MRO considered compliance history in determining the disposition track. relevant prior noncompliance with CIP-008-3 R1 includes a prior moderate risk violation of CIP-008-3 R1 (CIP-008-3 R1 includes a prior moderate risk violation of CIP-008-3 R1 includes a prior moderate risk violation risk.									
			In determining the penalty, MRO considered the investments that has made in its compliance program since the second s									
			conducted by third-party	Finally, the noncompliance compliance companies.	e was detected after named a new	w CIP Senior Manager, who undertoo	ok a review of CIP	program that include	ed two internal audits			