Federal Energy Regulatory Commission
Washington, D.C. 20426
August 30, 2021

Re: Thirty Second Determination Letter
FOIA No. FY19-30

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This is a response to your correspondence received in January 2020, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated August 20, 2021, the submitter and the concerned Unidentified Registered Entity (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. NP13-39, along with the name of a relevant URE inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney April D. Seabrook by email at april.seabrook@usdoj.gov, by phone at (202) 252-2525, or

[1] 5 U.S.C. § 552 (2018).

[2] This docket involved multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the UREs for whom FERC determined that disclosure of identities was appropriate.

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2021.08.30 11:31:38 -04'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

Peter Sorenson, Esq.
Counsel for Mr. Mabee
petesorenson@gmail.com

James M. McGrane
Senior Counsel
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, D.C. 20005
James.McGrane@nerc.net

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011278	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-005-1 R1. As part of a vendor assessment of its CIP compliance program, RFC_URE1 discovered that it failed to identify and protect certain devices that are Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter (ESP) pursuant to CIP-005-1 R1.5. RFC_URE1 utilizes its security event and incident management (SEIM) servers to aggregate security event logs from ESP access points and to issue automated alerts for the investigation of potential cybersecurity incidents. The SEIM system consists of collector servers and a logging database server, and RFC_URE1 failed to afford these servers certain of the protective measures required by CIP-005-1 R1.5. Specifically, RFC_URE1 failed to afford the SEIM servers the protections of CIP-003-1 R6, CIP-006-1 R3, and CIP-007-1 R3, R4, R5, R6, and R9.	CIP-005-1	R1; R1.5	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Reliability*First* determined that the violation posed a moderate risk because it implicated a significant class of assets that could pose a threat to the ESP, is not a documentation error, and spans a lengthy duration. The risk posed to the BPS was mitigated by the following factors. The SEIM system is located within RFC_URE1's staffed corporate data center that has controlled access in place. RFC_URE1 afforded the SEIM servers certain protective measures, including the protective measures of CIP-003-1 R1 through R5, CIP-004-1 R3, CIP-005-1 R2 and R3, CIP-007-1 R1, R7, and R8, CIP-008-1, and CIP-009-1. Specifically, RFC_URE1 had the following: a documented personnel risk assessment program, organizational processes and technical and procedural mechanisms for control of electronic access, electronic or manual processes for continuous monitoring and logging access, test procedures, established formal methods, processes, and procedures for disposal or redeployment of Cyber Assets used in the access control and monitoring of the ESP, as identified and documented in Standard CIP-005, and annual performance of a cyber vulnerability assessment.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011280	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First,* stating that it was in violation of CIP-006-1 R1.8. As part of a vendor assessment of its CIP compliance program, RFC_URE1 discovered that it failed to afford certain protective measures to Cyber Assets used to authorize and/or log access to the Physical Security Perimeter (PSP) pursuant to CIP-006-1 R1.8. RFC_URE1 utilizes specific operator workstations for badge creation and provisioning, user access rights management, monitoring alarms related to the PSP, and remote control of lock mechanisms. RFC_URE1 failed to afford these workstations certain protective measures specified in CIP-006-1 R1.8. Specifically, RFC_URE1 failed to ensure that it protected these workstations from unauthorized physical access and failed to afford these workstations the protections of CIP-003-1 R6 and CIP-007-1 R1, R2, R3, R6, R7, and R9.	CIP-006-1	R1; R1.8	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Reliability*First* determined that the violation posed a moderate risk because a violation of CIP-006-1 R1.8 provides the opportunity to access the PSP by leaving Cyber Assets that authorize and/or log access to the PSP unprotected. The risk posed to the BPS by the foregoing facts and circumstances was mitigated by the following factors. The workstations are located within secured buildings with controlled access. RFC_URE1 protected the workstations with user identifications and passwords, and access was limited to those who have personnel risk assessments and cybersecurity training. RFC_URE1 afforded the workstations certain protective measures, including the protective measures of CIP-003-1 R1 through R5, CIP-004-1 R3, CIP-005-1 R2 and R3, CIP-006-1 R4 and R5, CIP-007-1 R4, R5, and R8, CIP-008-1, and CIP-009-1. Specifically, RFC_URE1 had: a documented personnel risk assessment program, organizational processes and technical and procedural mechanisms for control of electronic access, electronic or manual processes for monitoring and logging access, operational and procedural controls to continuously manage physical access, technical and procedural controls for continuous monitoring of physical access, a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches, anti-virus software and other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware, technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access, established formal methods, processes, and procedures for disposal or redeployment as identified and documented in Standard CIP-005, annual performance of a cyber vulnerability assessment, and a cybersecurity incident response plan and implement the plan in response to cybersecurity incidents; and recovery plans for the subject assets. Furthermore, RFC_URE1 implements several other security solutions designed to minimize overall cybersecurity and physical security risk, including intrusion detection, anti-virus, security logging, and access control.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the Standard became mandatory and enforceable for RFC_URE1	Mitigation Plan completion	$0 (for RFC2012011278 and RFC2012011280)	Self-Report	To mitigate this violation, RFC_URE1: 1) added the devices to the list of Cyber Assets such to ensure that SEIM servers are identified as Cyber Assets used in the access control and/or monitoring of the ESP; that they are have become subject to the same requirements as applied to other Cyber Assets and applied the protections required by CIP-005-3a R1.5; 2) ensured that appropriate change management procedures are used to manage changes to SEIM servers per CIP-003-3 R6; 3) moved the SEIM servers within an identified Physical Security Perimeter per CIP-006-3 R3; 4) ensured that appropriate security posture verification is performed on SEIM servers for significant changes per CIP-007-3 R1; 5) developed a baseline of required ports and services for SEIM servers and ensured that the baseline is monitored per CIP-007-3 R2; 6) verified that the SEIM servers are included in RFC_URE1's corporate security patch management program and that all related documentation is in place per CIP-007-3 R3; 7) implemented anti-virus software or submitted Technical Feasibility Exception documentation for the SEIM servers as necessary per CIP-007-3 R4; 8) verified that all shared accounts used to administer the SEIM servers are managed according to the company's NERC CIP shared account management procedure per CIP-007-3 R5; 9) verified that appropriate security status monitoring is performed for the SEIM servers per CIP-007-3 R6; 10) ensured that any disposal or redeployment activity related to SEIM servers follows the company's NERC CIP Cyber Asset disposal or redeployment procedure per CIP-007-3 R7; 11) ensured that vulnerability assessments have been performed for SEIM servers per CIP-007-3 R8; 12) updated procedures related reviewing and updating documentation per CIP-007-3 R9; and 13) ensured that support personnel for the SEIM servers received appropriate training and awareness information related to the classification of the servers as Cyber Assets.	11/15/2012	4/3/2013	Admits	Reliability*First* reviewed RFC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. Reliability*First* also considered that it discovered the violations through Self-Reports and applied mitigating credit. RFC_URE1 promptly reported these violations as a result of the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. Reliability*First* seeks to encourage this type of behavior including self-reporting characterized by spontaneous timely correction unconnected to a pending regional compliance monitoring action and periodic outside examination of the compliance program, by imposing a zero dollar monetary penalty for these violations.
when the Standard became mandatory and enforceable for RFC_URE1	Mitigation Plan completion	$0 (for RFC2012011278 and RFC2012011280)	Self-Report	To mitigate this violation, RFC_URE1: 1) added the devices to the list of Cyber Assets such that they have become subject to the same requirements as applied to other Cyber Assets and applied the protections required by CIP-006-3c R2.2; 2) updated the company's CIP-006 compliance procedures to ensure that operator workstations (for NERC CIP PSP functions) were identified as Cyber Assets used in the access control and/or monitoring of the PSP; 3) identified workstations which were, or could have been, used as operator workstations for NERC CIP PSP functions, but are not needed and identified as Cyber Assets in item 1 above, and removed or restricted functionality that was not needed on such workstations, 4) ensured that appropriate change management procedures are used to manage changes to operator workstations per CIP-003-3 R6; 5) implemented measures to ensure that the operator workstations are protected from unauthorized physical access per CIP-006-3 R2.1; 6) ensured that appropriate security posture verification is performed on operator workstations for significant changes per CIP-007-3 R1; 7) developed a baseline of required ports and services for operator workstations and ensured that the baseline is monitored per CIP-007-3 R2; 8) verified that the operator workstations are included in the corporate security patch management program and that all related documentation is in place per CIP-007-3 R3; 9) implemented anti-virus software on the operator workstations as necessary per CIP-007-3 R4; 10) verified that all shared accounts used to administer operator workstations are managed according to the company's NERC CIP shared account management procedure per CIP-007-3 R5; 11) verified that appropriate security status monitoring is performed for the operator workstations per CIP-007-3 R6; 12) ensured that any disposal or redeployment activity related to operator workstations follows the company's NERC CIP Cyber Asset disposal or redeployment procedure per CIP-007-3 R7; 13) ensured that vulnerability assessments have been performed for operator workstations per CIP-007-3 R8; 14) updated procedures related reviewing and updating documentation per CIP-007-3 R9; and 15) ensured that support personnel for the operator workstations received appropriate training and awareness information related to the classification of the workstations as Cyber Assets.	11/15/2012	4/3/2013	Admits	Reliability*First* reviewed RFC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. Reliability*First* also considered that it discovered the violations through Self-Reports and applied mitigating credit. RFC_URE1 promptly reported these violations as a result of the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. Reliability*First* seeks to encourage this type of behavior including self-reporting characterized by spontaneous timely correction unconnected to a pending regional compliance monitoring action and periodic outside examination of the compliance program, by imposing a zero dollar monetary penalty for these violations.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) Alcoa Power Generating, Inc. - Tapoco Division (APGI-Tapoco)	NCRXXXXX	SERC2013012141	Settlement Agreement	SERC_URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R1 because it had a deficient risk-based assessment methodology (RBAM) which it used to identify its Critical Assets. Specifically, SERC_URE1's RBAM failed to include evaluation criteria to determine if an asset considered pursuant to CIP-002-1 R1.2 was in fact a "Critical Asset," as that term is defined in the NERC Glossary of Terms. The SERC_URE1 RBAM evaluated whether a control center was a Critical Asset by asking whether there would be a loss of central control and/or situational awareness of SERC_URE1's operations in the event that the control center was severely damaged, destroyed, compromised, or misused. Using this criterion, SERC_URE1 applied its RBAM and identified certain control centers as Critical Assets. SERC_URE1 revised its RBAM by adding two additional questions to its evaluation criteria to determine whether a control center was a Critical Asset. The first question asked whether the failure, misuse, or compromise of a control center would result in a negative impact to the reliability of the Bulk Electric System (BES). The second question asked whether the failure or misuse of a control center would significantly impact a third party's Critical Asset. Pursuant to its revised RBAM, SERC_URE1 would determine that a control center was a Critical Asset only if the answer was "yes" to the original evaluation criterion and "yes" to one or both of the two additional evaluation criteria. Using these new criteria, SERC_URE1 applied its revised RBAM and determined that the control centers were not Critical Assets. The NERC Glossary of Terms defines the term "Critical Assets" as "[f]acilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Based on this definition, SERC determined that SERC_URE1's previous RBAM lacked sufficient evaluation criteria to determine if an asset considered pursuant to CIP-002-1 R1.2 was in fact a Critical Asset. Instead, the evaluation criterion that SERC_URE1 used was overly broad and resulted in the incorrect identification of assets as Critical Assets, when in fact those assets did not meet the definition of "Critical Assets" set forth in the NERC Glossary of Terms. SERC determined that the control centers should never have been identified as Critical Assets because they failed to meet the definition of that term.	CIP-002-1	R1; R1.1	Lower	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1's RBAM used an overly broad evaluation criterion that would result in the incorrect identification of certain assets as Critical Assets, resulting in extra protection for those assets and any associated Cyber Assets. SERC_URE1 conducted engineering studies and consulted with the registered entities it connects to in order to determine whether the control centers should be considered Critical Assets. SERC_URE1 determined that the loss or misoperation of all of the generation and transmission assets it controls and monitors with the control centers would not result in a negative impact to the reliability or operability of the BES. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2) Alcoa Power Generating, Inc. - Yadkin Division (APGI-Yadkin)	NCRXXXXX	SERC2013012139	Settlement Agreement	SERC_URE2 submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R1 because it had a deficient risk-based assessment methodology (RBAM) which it used to identify its Critical Assets. Specifically, SERC_URE2's RBAM failed to include evaluation criteria to determine if an asset considered pursuant to CIP-002-1 R1.2 was in fact a "Critical Asset," as that term is defined in the NERC Glossary of Terms. The SERC_URE2 RBAM evaluated whether a control center was a Critical Asset by asking whether there would be a loss of central control and/or situational awareness of SERC_URE2's operations in the event that the control center was severely damaged, destroyed, compromised, or misused. Using this criterion, SERC_URE2 applied its RBAM and identified certain control centers as Critical Assets. SERC_URE2 revised its RBAM by adding two additional questions to its evaluation criteria to determine whether a control center was a Critical Asset. The first question asked whether the failure, misuse, or compromise of a control center would result in a negative impact to the reliability of the Bulk Electric System (BES). The second question asked whether the failure or misuse of a control center would significantly impact a third party's Critical Asset. Pursuant to its revised RBAM, SERC_URE2 would determine that a control center was a Critical Asset only if the answer was "yes" to the original evaluation criterion and "yes" to one or both of the two additional evaluation criteria. Using these new criteria, SERC_URE2 applied its revised RBAM and determined that the control centers were not Critical Assets. The NERC Glossary of Terms defines the term "Critical Assets" as "[f]acilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Based on this definition, SERC determined that SERC_URE2's previous RBAM lacked sufficient evaluation criteria to determine if an asset considered pursuant to CIP-002-1 R1.2 was in fact a Critical Asset. Instead, the evaluation criterion that SERC_URE2 used was overly broad and resulted in the incorrect identification of assets as Critical Assets, when in fact those assets did not meet the definition of "Critical Assets" set forth in the NERC Glossary of Terms. SERC determined that the control centers should never have been identified as Critical Assets because they failed to meet the definition of that term.	CIP-002-1	R1; R1.1	Lower	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2's RBAM used an overly broad evaluation criterion that would result in the incorrect identification of certain assets as Critical Assets, resulting in extra protection for those assets and any associated Cyber Assets. SERC_URE2 conducted engineering studies and consulted with the registered entities it connects to in order to determine whether the control centers should be considered Critical Assets. SERC_URE2 determined that the loss or misoperation of all of the generation and transmission assets it controls and monitors with the control centers would not result in a negative impact to the reliability or operability of the BES. SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the Standard became mandatory and enforceable for SERC_URE1	Mitigation Plan completion	$0	Self-Report	To mitigate this violation, SERC_URE1: 1) revised its RBAM to include evaluation criteria that examined the risk to the BES; and 2) applied its revised RBAM and determined that it had no Critical Assets.	12/28/2012	4/18/2013	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
when the Standard became mandatory and enforceable for SERC_URE2	Mitigation Plan completion	$0	Self-Report	To mitigate this violation, SERC_URE2: 1) revised its RBAM to include evaluation criteria that examined the risk to the BES; and 2) applied its revised RBAM and determined that it had no Critical Assets.	12/28/2012	4/18/2013	Neither Admits nor Denies	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC201000561	Settlement Agreement	SERC_URE3 submitted a Self-Report to SERC stating it was in violation of CIP-007-2 R5 because it did not enforce access authentication of, and accountability for, all user activity for a single Critical Cyber Asset (CCA), due to the unauthorized sharing of a username and password. A SERC_URE3 technician supervisor gave two other technicians the supervisor's username and password to access the Energy Management System (EMS). The technicians shared the supervisor's username and password on one CCA workstation that had the EMS client installed, which SERC_URE3 used for troubleshooting Supervisory Control and Data Acquisition communications issues. The technicians engaged in this behavior in order to monitor the EMS continuously, as switching accounts between individual users was time consuming. This unauthorized sharing of the supervisor's username and password created a situation in which SERC_URE3 could not authenticate which individual was using the supervisor's account. The two technicians requested that the EMS supervisor create user accounts for them on the EMS. This request triggered a SERC_URE3 investigation that discovered the account sharing. A system administrator changed the technician supervisor's password to end the account sharing. SERC_URE3 completed its investigation and determined that there were no other instances of user passwords being shared. SERC_URE3 was unable to determine the exact start date of the violation.	CIP-007-1	R5	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The unauthorized access was limited to two SERC_URE3 employees who had completed cyber security training, had valid personnel risk assessments, and were authorized to access the CCA using their own credentials. The CCA is located in a room that is monitored by a video camera and requires scanning an access badge to both enter and exit the room, making identification of the CCA users possible. The unauthorized access was limited to on CCA. Finally, SERC_URE3's investigation did not reveal any unauthorized activity on the account.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2011008332	Settlement Agreement	SERC_URE3 submitted a Self-Report to SERC stating it was in violation of CIP-006-3c R2.2, because it did not perform an annual cyber vulnerability assessment (CVA) of Physical Access Control Systems (PACS) devices. SERC_URE3 did not include a review of its PACS devices in its annual CVAs, extending this issue back to Version 1 of the Standard. SERC_URE3 discovered this violation when it conducted an internal review of its PACS device compliance. SERC_URE3's review revealed that it had not afforded its PACS devices the protective measures specified in CIP-007-1 R8. Specifically, SERC_URE3 had not conducted annual cyber vulnerability testing on its PACS devices. SERC_URE3's PACS devices included one door access system consisting of servers and control panels. SERC_URE3 included these PACS devices in the CVA it had previously completed.	CIP-006-1	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's PACS were on a separate interface that limited user access and disabled all external internet connectivity. SERC_URE3 had an independent door access system that protected access to the building which contained identified Physical Security Perimeters (PSPs) and was protected within a secured area. SERC_URE3's internal review revealed that it had afforded its PACS devices all other protective measures required by CIP-006-1 R1.8. Finally, SERC_URE3 did not identify any PACS device vulnerabilities in its CVA.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the Standard became mandatory and enforceable for SERC_URE3	when SERC_URE3 changed the supervisor's password to end the unauthorized access	$5,000 (for SERC201000561 and SERC2011008332)	Self-Report	To mitigate this violation, SERC_URE3: 1) counseled all affected employees as to the proper manner of sharing computer terminals; 2) disciplined the EMS technicians pursuant to SERC_URE3's corporate discipline system; and 3) acquired additional workstations with licenses to enable more technicians to be able to log into and lock out their respective workstations without affecting the performance of the other technicians.	10/27/2010	3/18/2013	Admits	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
the day after SERC_URE3 should have conducted its annual CVA including PACS devices)	when SERC_URE3 completed its CVA including PACS devices	$5,000 (for SERC201000561 and SERC2011008332)	Self-Report	To mitigate this violation, SERC_URE3: 1) completed a CVA for PACS devices; 2) ensured that PACS devices would be included in CVAs in the future; and 3) completed a CVA for the following year, which included the PACS devices.	12/31/2012	2/28/2013	Admits	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102616	Settlement Agreement	WECC_URE1 submitted a Self-Report to WECC stating that it was in violation of CIP-004 R3 because an employee was granted authorized unescorted physical access to Critical Cyber Assets (CCAs) without having a personnel risk assessment (PRA). The employee was given unescorted access to WECC_URE1's control center for one day.	CIP-004-3	R3	Medium	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, for one person, WECC_URE1 failed to conduct a PRA prior to granting that person access to CCAs, for one day. As a compensating measure, the individual having access had been a WECC_URE1 contractor for about seven years and had cybersecurity training. WECC_URE1 had twenty-four hour logging and monitoring of physical and electronic access in place at the facility.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102901	Settlement Agreement	During a Compliance Audit, WECC discovered that WECC_URE1 was in violation of CIP-005-1 R2 because it failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter (ESP). Specifically, WECC_URE1 did not enable only ports and services required for operations and for monitoring its Cyber Assets within its ESP. Also, WECC discovered that WECC_URE1 was in violation of CIP-005-1 R2.4 because it did not implement strong procedural or technical controls to ensure authenticity at the access points to its ESPs where there was external interactive access. In addition, WECC discovered that WECC_URE1 was in violation of CIP-005-1 R2.6 because it did not display an appropriate use banner on its associated user screen upon all access attempts.	CIP-005-1	R2; R2.4; R2.6	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC determined that the violation posed a moderate risk because the use of non-restrictive rules on the firewalls allows for potential malicious activities from a source to a destination device. This activity could have resulted in compromise, degradation of performance, and possible denial of service of an asset. Interactive access to a device within an ESP must always provide a warning banner to ensure that the user is knowledgeable that the asset they are connected to is for restricted access only. The lack of strong controls at the access point for all traffic entering the ESP allows direct access to a device prior to formal authorization. The risk was mitigated because WECC_URE1 authenticates all access prior to network access.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102902	Settlement Agreement	During a Compliance Audit, WECC discovered that WECC_URE1 was in violation of CIP-006-1 R1.8 because it did not afford Cyber Assets used in the access control and monitoring of the Physical Security Perimeter, the protective measures specified in CIP-007 R5.3.2 and R5.3.3. Specifically, WECC_URE1 stated in response to a data request that "passwords have not been changed for account users annually," as required by CIP-007-1 5.3.3. In addition, WECC discovered that at least one employee with access to WECC_URE1's system did not have passwords that consisted of a combination of alpha, numeric, and "special characters" required in CIP-007 R5.3.2.	CIP-006-1	R1.8	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. As a mitigating factor, WECC_URE1 had twenty-four hour logging and monitoring of physical and electronic access in place at all facilities, including the facility involved in this violation.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the employee was granted unescorted physical access	when the employee's unescorted physical access was terminated	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Self-Report	To mitigate this violation, WECC_URE1: 1) performed a PRA for the employee; 2) implemented procedures to minimize errors; and 3) upgraded permissions to gain access to its critical facilities.	5/5/2011	6/30/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. A Settlement Agreement covering violations of CIP-004-1 R3 for WECC_URE1 was filed with FERC under NP11-140-000 on March 30, 2011. On April 29, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. WECC determined that this prior violation should not serve as a basis for aggravating the penalty. The conduct of the prior violation was not the same or similar to the instant violation.
when the Standard became mandatory and enforceable for WECC_URE1	Mitigation Plan completion	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) configured its firewall to block and prevent applications and services through its ESP access points; 2) replaced the firewall with another firewall with the ability to implement the security policies; 3) established procedural controls at firewall access points to ensure authenticity of the accessing party; and 4) added acceptable use banners to firewall access points.	12/11/2012	2/25/2013	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
when the Standard became mandatory and enforceable for WECC_URE1	Mitigation Plan completion	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) updated its system with complex passwords that consist of a combination of alpha, numeric, and special characters; and 2) established a compliance tracking and management tool to ensure that passwords are changed annually, or more frequently, based on risk.	12/11/2011	1/26/2012	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102859	Settlement Agreement	WECC_URE1 submitted a Self-Report to WECC stating that it was in violation of CIP-006 R1.4 because it did not use physical access controls as described in R4, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. One contract employee was given physical access without having CIP training.	CIP-006-3c	R1.4	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. As a mitigating factor, WECC_URE1 had twenty-four hour logging and monitoring of physical and electronic access in place at all facilities, including the facility involved in this violation.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102903	Settlement Agreement	During a Compliance Audit, WECC discovered that WECC_URE1 was in violation of CIP-006-1 R3 because it failed to have alarms to indicate a door, gate, or window has been opened without authorization and provide immediate notification to personnel responsible for response. Specifically, WECC_URE1 failed to monitor physical access at five access points (three Critical Asset locations) to the Physical Security Perimeter (PSP) twenty-four hours a day, seven days a week.	CIP-006-1	R3	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The failure to have alarms that provide for an immediate response could allow unauthorized individuals access to WECC_URE1's PSP. If an unauthorized individual gained access to WECC_URE1's PSP, that person could use that access to engage in malicious conduct and cause damage to WECC_URE1's system. As a mitigating factor, WECC_URE1 had twenty-four hour logging and monitoring of physical and electronic access in place at all facilities, including the facility involved in this violation.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102904	Settlement Agreement	During a Compliance Audit, WECC discovered that WECC_URE1 was in violation of CIP-007-1 R5. Specifically, WECC_URE1 did not provide sufficient evidence to demonstrate that it renamed administrator and factory default accounts as required by CIP-007-1 R5.2.1. In addition, WECC_URE1 did not provide sufficient evidence to establish that it identified individuals with access to shared accounts as required by CIP-007 R5.2.2. The Audit team did not find evidence of an audit trail of the shared account use, automated or manual.	CIP-007-1	R5	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was mitigated because WECC_URE1 had an account management policy in place, even though it was not implemented completely.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the contract employee was first given physical access	when the contract employee's access was removed	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Self-Certification	To mitigate this violation, WECC_URE1: 1) revoked the access of the individual involved; and 2) implemented a procedure that acts as a double-check on access rights to prevent future inadvertent granting of access rights.	7/14/2011	7/20/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
when the Standard became mandatory and enforceable for WECC_URE1	Mitigation Plan completion	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) established operational requirements for its physical security system that define the operation and alarming of access points at PSPs; 2) installed door alarms, including door held open and forced entry alarms on the doors cited in the violation; 3) established procedures for response to events/alarms and trained users and maintainers of the system on the new security system functionality and features; 4) updated its Physical Security Procedures and Plan document and other security system documentation; and 5) developed system test procedures and maintenance forms to assure proper system operation.	3/22/2012	6/21/2012	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
when the Standard became mandatory and enforceable for WECC_URE1	Mitigation Plan completion	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) reviewed its account management procedure; 2) determined the number of shared or generic accounts on its system and determined the number of individuals with access to shared or other generic accounts; 3) removed shares to other generic accounts; 4) implemented an audit trail for use of shared accounts; and 5) implemented an manual process for capturing shared account use.	8/31/2012	9/21/2012	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102905	Settlement Agreement	During a Compliance Audit WECC discovered that WECC_URE1 was in violation of CIP-007-1 R8 because it did not perform a cyber vulnerability assessment (CVA) of all Cyber Assets within the Electronic Security Perimeter (ESP) at least annually and did not perform the CVA per the requirements of the Standard. In addition, WECC_URE1's CVA for other calendar years did not include all Critical Cyber Assets (CCAs) within its ESP. Also, WECC_URE1 did not provide sufficient evidence to demonstrate that only those ports and services required for operation of the Cyber Assets within the ESP were reviewed and enabled. Finally, WECC_URE1 did not document action plans to remediate or mitigate vulnerabilities identified in the an assessment.	CIP-007-1	R8	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk was mitigated because WECC_URE1 had an account management policy. WECC_URE1 performed vulnerability assessments in past years and would have been able to address vulnerabilities during the year prior to and after the year it failed to perform the vulnerability assessment.

Attachment A-2

May 30, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
when the Standard became mandatory and enforceable for WECC_URE1	Mitigation Plan completion	$62,500 (for WECC201102616, WECC201102901, WECC201102902, WECC201102859, WECC201102903, WECC201102904, and WECC201102905)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) updated its vulnerability assessment process document; 2) trained technical personnel on the activities and documentation necessary to perform a compliant vulnerability assessment; 3) performed a CVA of all CCAs based on its updated vulnerability assessment process document; and 4) established a yearly task for a CVA.	5/30/2012	7/10/2012	Agrees/ Stipulates	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

Document Accession #: 20130531-5384 Filed Date: 05/31/2013

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 31, 2013

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: NERC Spreadsheet Notice of Penalty Filing – Errata
FERC Docket No. NP13-39-000

On May 30, 2013, the North American Electric Reliability Corporation (NERC) submitted a Spreadsheet Notice of Penalty filing. It has come to NERC's attention that the NERC violation ID number associated with one of the violations was incorrect. Specifically, the violation ID number associated with SERC Unidentified Registered Entity 1 should be SERC2013012141 instead of SERC2013012139. NERC's instant filing includes, in Attachment A, a revised Spreadsheet Notice of Penalty reflecting the correction.

Request for Confidential Treatment

Attachment A includes confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standards possible violations and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the information in the attached documents is deemed "confidential" by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

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

Please contact the undersigned with any questions regarding the submittal.

Respectfully submitted,

/s/ Edwin Kichline
Edwin Kichline
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation

Enclosures: Attachment A

Document Accession #: 20130531-5384 Filed Date: 05/31/2013

Document Content(s)