September 28, 2017

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement to resolve all outstanding issues arising from SERC's determination and findings of 59 total violations, including 50 violations of Critical Infrastructure Protection (CIP) Reliability Standards and 9 violations of the Operations and Planning NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

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

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

According to the Settlement Agreement, URE admits to the violations and agrees to the assessed penalty of five hundred thousand dollars ($500,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

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

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012661	CIP-002-3	R3	High/ Severe	CA	Serious	$500K
SERC2016015522	CIP-002-3	R4	Lower/ Severe	SR	Moderate	
SERC2013012662	CIP-003-3	R1; R1.3	Medium/ Severe	CA	Moderate	
SERC2013012663	CIP-003-3	R6	Lower/ Severe	CA	Moderate	
SERC2013012664	CIP-004-3	R2; R2.1	Medium/ Severe	CA	Moderate	
SERC2013012665	CIP-004-3	R3	Medium/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016016616	CIP-004-3	R3; R3.3	Medium/ Moderate	SR	Moderate	
SERC2016015515	CIP-004-3a	R3; R3.2	Medium/ Moderate	SR	Minimal	
SERC2013012666	CIP-004-3	R4	Lower/ Severe	CA	Moderate	
SERC2016015480	CIP-004-3a	R4; R4.2	Lower/ Moderate	SR	Minimal	
SERC2016016615	CIP-004-6	R5; R5.2	Medium/ Moderate	SR	Minimal	
SERC2017016813	CIP-004-6	R5; R5.4	Medium/ Lower	SR	Minimal	
SERC2013012667	CIP-005-3	R1; R1.1; R1.5	Medium/ Severe	CA	Serious	$500K
SERC2016016619	CIP-005-3a	R1	Medium/ Severe	SR	Moderate	
SERC2017017849	CIP-005-3a	R1; R1.1	Medium/ Severe	SR	Moderate	
SERC2013012668	CIP-005-3	R2; R2.2; R2.4	Medium/ Severe	CA	Serious	
SERC2016016620	CIP-005-3a	R2; R2.2	Medium/ Severe	SR	Moderate	
SERC2013012669	CIP-005-3	R4; R4.2; R4.3; R4.4	Medium/ Severe	CA	Moderate	
SERC2013012670	CIP-005-3	R5; R5.1; R5.2	Lower/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016015523	CIP-005-3a	R5; R5.1	Lower/ Severe	SR	Moderate	$500K
SERC2013012671	CIP-006-3a	R1; R1.2; R1.8	Medium/ Severe	CA	Moderate	
SERC2016015516	CIP-006-3c	R1; R1.6	Medium/ Severe	SR	Serious	
SERC2016015524	CIP-006-3c	R1; R1.8	Lower/ Severe	SR	Moderate	
SERC2016016603	CIP-006-6	R1; R1.3	Medium/ Severe	SR	Moderate	
SERC2013012678	CIP-006-3a	R2	Medium/ Severe	CA	Moderate	
SERC2016016606	CIP-006-6	R2; R2.1	Medium/ Severe	SR	Minimal	
SERC2016016611	CIP-006-6	R2; R2.2	Medium/ Severe	SR	Minimal	
SERC2017017812	CIP-006-6	R2; R2.2	Medium/ Severe	SR	Minimal	
SERC2013012681	CIP-007-3a	R2; R2.1; R2.2; R2.3	Medium/ Severe	CA	Moderate	
SERC2013012675	CIP-007-3a	R3; R3.1; R3.2	Lower/ Severe	CA	Serious	
SERC2013012676	CIP-007-3a	R4; R4.1	Medium/ Severe	CA	Minimal	
SERC2013012677	CIP-007-3a	R5; R5.1.2; R5.3	Lower/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012680	CIP-007-3a	R6; R6.1	Lower/ Severe	CA	Minimal	
SERC2013012679	CIP-007-3a	R8; R8.2; R8.3	Lower/ Severe	CA	Moderate	
SERC2016015525	CIP-007-3a	R9	Lower/ Severe	SR	Moderate	
SERC2017017851	CIP-007-6	R2; R2.1	Medium/ Moderate	SR	Minimal	
SERC2016016614	CIP-007-6	R2; R2.2	Medium/ Lower	SR	Minimal	
SERC2016016609	CIP-007-6	R2; R2.3	Medium/ High	SR	Minimal	
SERC2017017811	CIP-007-6	R2; R2.4	Medium/ Severe	SR	Moderate	$500K
SERC2017017813	CIP-007-3a	R6; R6.1	Medium/ Severe	SR	Minimal	
SERC2016016605	CIP-007-6	R4; R4.4	Medium/ Lower	SR	Minimal	
SERC2017017854	CIP-007-3a	R5; R5.2.1	Lower/ Severe	SR	Moderate	
SERC2016016607	CIP-007-3a	R5; R5.3.3	Lower/ Severe	SR	Moderate	
SERC2016016608	CIP-007-6	R5; R5.5	Medium/ High	SR	Minimal	
SERC2016016610	CIP-007-6	R5; R5.7	Medium/ Severe	SR	Minimal	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012682	CIP-009-3	R1	Medium/ Severe	CA	Moderate	$500K
SERC2017017850	CIP-010-2	R1; R1.1	Medium/ Severe	SR	Minimal	
SERC2016016612	CIP-010-2	R1; R1.3	Medium/ Severe	SR	Moderate	
SERC2017017852	CIP-010-2	R1; R1.5	Medium/ Severe	SR	Moderate	
SERC2016016613	CIP-010-2	R2; R2.1	Medium/ Severe	SR	Moderate	
SERC2016015460	BAL-002-1	R4	Medium/ Severe	PDS	Minimal	
SERC2016016157	BAL-003-1.1	R2	Medium/ Severe	SR	Minimal	
SERC2016015526	FAC-014-2	R3	Medium/ Severe	SR	Minimal	
SERC2016015527	FAC-014-2	R4	Medium/ Severe	SR	Minimal	
SERC2017016808	PRC-002-2	R5; R5.3	Lower/ Severe	SR	Minimal	
SERC2016015697	PRC-023-3	R6	High/ Severe	SR	Minimal	
SERC2016015532	TPL-002-0b	R1; R1.3	High/ Lower	SR	Minimal	
SERC2016015533	TPL-003-0b	R1; R1.3	High/ Lower	SR	Minimal	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016015534	TPL-004-0a	R1; R1.3	Medium/ Lower	SR	Minimal	$500K

FACTS COMMON TO VIOLATIONS

During a Compliance Audit, SERC determined that URE had multiple violations of the CIP Reliability Standards. Following the Compliance Audit, URE's initial responses to SERC's requests for information (RFIs) were only partially responsive to the questions asked. SERC attempted to resolve the noncompliance with URE. URE provided SERC with draft Mitigation Plans a year after the audit, but did not submit formal plans until two years after the audit. SERC staff conducted multiple on-site visits in order to validate URE's completion of Mitigation Plan milestones and the completion of Mitigation Plans. Three years after the audit, URE submitted an additional series of Self-Reports covering violations of both Operations and Planning Reliability Standards and CIP Reliability Standards.

Due to the poor quality of the evidence provided to SERC staff during the on-site visits, SERC staff was only able to validate that URE completed one-fifth of its Mitigation Plans. SERC staff ended the last on-site visit early because of the significant and repeated difficulties the SERC on-site team had in verifying Mitigation Plan completion using the evidence that URE presented. As a result, SERC issued a Notice of Alleged Violation and required URE to submit new Mitigation Plans for the violations that SERC staff was unable to verify.

Shortly thereafter, SERC and URE agreed to URE's working with an external team of advisors to help it identify any additional cybersecurity risks, develop adequate Mitigation Plans to address the existing violations and any new violations, and provide sufficient evidence to demonstrate compliance. This team of advisors' work resulted in additional CIP Self-Reports and Operations and Planning Self-Reports.

SERC determined that, while the risk posed to the bulk power system (BPS) by the individual violations ranged from minimal to serious, the collective risk of the 59 violations posed a serious risk to the reliability of the BPS. URE's violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS primarily because of the lengthy duration of the unmitigated risk.

Critical Infrastructure Protection Violations

URE's violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS primarily because of the lengthy duration the violations went on without mitigation. As one example, URE's failures relating to identifying and documenting its Critical Cyber Assets (CCAs) could result in incomplete or inaccurate documentation of the Electronic Security Perimeter (ESP) and associated Cyber Assets, which could lead personnel to take incorrect actions based on outdated or missing information. There were also failures across the CIP standards relating to lack of awareness, engagement, and accountability for CIP compliance. URE did have some protections in place to protect the reliability of the BPS. Specifically, URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP for unusual activity.

SERC2013012661 CIP-002-3 R3 - OVERVIEW

SERC determined that URE failed to develop a list of CCAs that included all CCAs essential to the operation of the Critical Assets. Specifically, URE excluded eight assets comprising a virtual storage infrastructure that it failed to identify and document as CCAs that were essential to the operation of a Critical Asset.

The cause of this violation was inadequate processes and procedures to identify CIP assets.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to identify, document, and protect the devices as CCAs could have led to unauthorized access, data loss, or the failure of operator workstations, which could disrupt URE's situational awareness of the BPS. Several factors increased the risk of the violation. First, the vendor personnel in URE's CIP-004 violations, described below, had electronic access to the devices, but URE had not ensured that those individuals had completed cybersecurity training or had valid personnel risk assessments (PRAs), and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. URE had no means of ensuring the authenticity of the vendor personnel accessing the devices from outside the ESP, who were able to use a URE shared account to make changes to those devices remotely. Second, URE also did not provide any of the CIP-007 protections to the devices, and the management interface was outside of the ESP. Third, URE did not have a documented network asset backup procedure which could be used to recover the devices. Some factors provided some degree of protection. URE protected the connections inside the ESP and inside a Physical Security Perimeter (PSP). Also, while the misuse or failure of the devices could prevent

URE personnel from initially logging onto a workstation, it would not prevent URE personnel from continuing to use a workstation on which they had already been working.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed Critical Assets needed to support the Bulk Electric System (BES) and created the initial CIP asset list identifying BES Cyber Assets, Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs), and Electronic Access Control or Monitoring Systems (EACMS), which was signed by the CIP senior manager;
2. Created an asset management process to address the identification and documentation of BES Cyber Systems and the underlying CIP Assets comprising the BES Cyber Systems;
3. Implemented a URE CIP asset classifications procedure;
4. Completed an annual review of all URE assets to ensure not only the proper classification of URE CIP Assets, but also a review of those that are not identified as CIP Assets; and
5. Conducted training on the new procedures and identification of CIP Assets generally.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015522 CIP-002-3 R4 - OVERVIEW

SERC determined that URE failed to approve the risk-based assessment methodology (RBAM), the list of Critical Assets, and the list of CCAs annually in one year.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual approval, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to annually approve the RBAM, Critical Asset list, and CCA list could have resulted in failures to document changes in the RBAM or failures to assess and document whether all relevant facilities or Cyber Assets should be identified as Critical Assets or CCAs. The risk of this violation was elevated by similar URE failures to review documentation annually in NERC Violation IDs SERC2016015523 (CIP-005-3 R5), SERC2016015524 (CIP-006-3 R1.8), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and

compliance with the CIP Standards. Nevertheless, this violation represented a failure to review documentation annually and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from the date the URE failed to annually approve its RBAM through when URE's CIP senior manager signed and approved the RBAM.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had its CIP senior manager approve the RBAM;
2. Created, as a part of a renewed focus on managing documentation, a relevant department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP program. Job descriptions for those staffing positions include references to their role in document management; and
3. In order to track and manage deadlines, had its new IT department build a document management database that tracks review dates and will trigger notifications for reviews and updates to business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012662 CIP-003-3 R1; R1.3 - OVERVIEW

SERC determined that URE failed to demonstrate that its senior manager annually reviewed and approved its cybersecurity policy after its creation for approximately five years.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual approval.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document the annual review and approval of the cybersecurity policy documents by the senior manager could result in URE personnel using an outdated version of the cybersecurity policy documents that did not adequately address current threats or the current state of URE's cybersecurity protections and procedures. Outdated cybersecurity policy documents could lengthen the period of time URE would need to respond to and recover from an emergency. Nevertheless, URE's cybersecurity policy documents are readily available to all personnel, and URE

requires employees to acknowledge the cybersecurity policy documents annually. In addition, contractors are required to acknowledge and to sign the cybersecurity policy documents annually.

SERC determined the duration of the violation to be approximately three years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Revised its administrative processes to require the CIP senior manager to approve, in writing, the policies relevant to URE's CIP Program. The policies are listed with the effective date for each, a statement from the CIP senior manager, and the date and signature of the CIP senior manager. This document will be part of the documentation URE reviews and approves annually; and
2. Had its CIP senior manager approve the cybersecurity policy.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012663 CIP-003-3 R6 - OVERVIEW

SERC determined that URE failed to provide evidence that it adequately documented changes to hardware components of certain CCAs pursuant to the requirements of its documented change control process. URE created change request documentation that had a generic change summary but did not specify the CCA hardware that was removed, redeployed, or returned to the vendor.

The cause of this violation was URE's inadequate change management process and controls.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement its documented change control process resulted in insufficient documentation of changes to CCA hardware components, which could lead to unauthorized changes to CCAs or the disposal of CCA hardware without following approved redeployment or disposal procedures, potentially resulting in the compromise of CCA information. Nevertheless, URE managed the redeployment of Cyber Assets and CCA hardware from the decommissioned site to the new site, and there was no third party involved. URE personnel were present with vendor personnel while CCA hardware was replaced.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Revised its Change Management processes and controls to require additional details regarding the move or replacement of hardware components. URE also enhanced its asset disposal process documentation similarly;
2. Implemented full change management processes and controls for all hardware replacements for these devices;
3. Had the URE compliance department provide training to the server administration department for using the change management process for all hardware replacements;
4. Revised a specific process document to specifically link URE's asset management system to the disposal manifest by using serial number as a common key to both processes;
5. Revised a specific process document to specifically include language for the disposal of certain equipment;
6. Provided training on the changes; and
7. Provided the historic documents showing that the devices were tracked and managed by URE during the move.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012664 CIP-004-3 R2; R2.1 - OVERVIEW

SERC determined URE failed to provide sufficient evidence to demonstrate that remote vendor personnel received cybersecurity training prior to receiving electronic access to four devices URE identified as CCAs, and did not identify the access by vendors as a specified circumstance for an exception.

The cause of this violation was URE's inadequate oversight and procedures relating to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that vendor personnel were trained on its cybersecurity training program could lead to poor security practices that could result in the compromise of the identified CCAs, including the energy management system (EMS), adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support

agreement with the vendor where the vendor personnel are to undergo stringent vetting, including criminal background check and identity verification. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Restricted external access by vendor support resources by programmatically disabling the vendor gateway. Vendor support resources can no longer access CCAs without URE's authorization;
2. Moved the URE server into the ESP;
3. Identified the three vendor resources who are allowed to access the URE equipment. These three resources have provided completed PRA certifications and security awareness training;
4. Had the vendor resources complete URE security awareness training;
5. Had the relevant URE supervisor inform the personnel on their team who manage the vendor gateway that only the three named vendor staff are allowed through the gateway to access the vendor equipment which URE owns; and
6. Implemented the capturing of audit logging from the vendor gateway. This allows staff to monitor and review all access by vendor support personnel.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012665 CIP-004-3 R3 - OVERVIEW

SERC determined that URE failed to document that PRAs of third-party vendors had occurred pursuant to CIP-004 prior to granting access to CCAs. The SERC audit team discovered that a third-party vendor had electronic access to four devices that URE had identified as CCAs. The vendor personnel had electronic access in order to provide remote support, but URE had not documented that the required PRAs had been performed prior to granting access.

The cause of this violation was URE's inadequate oversight and procedures related to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document that vendor personnel had completed PRAs meeting the requirements of CIP-004 R3 could lead to individuals with criminal backgrounds gaining access to and compromising identified CCAs, including the EMS, adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support agreement with the vendor where the vendor personnel are to undergo stringent vetting, including a criminal background check and identity verification. Based on information provided by the vendor, its background checks include drug testing, something that is not required by R3. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented the capturing of audit logging from the vendor gateway. This allows staff to monitor and review all access by vendor support personnel to the vendor management console;
2. Removed external access by vendor resources by turning off the support gateway. Vendor support resources can no longer access this data storage appliance without URE consent and subsequent enabling of the gateway to the management console;
3. Had the vendor provide certification of a PRA for local, dedicated vendor resources which complied with URE requirements;
4. Had the relevant URE supervisor inform the personnel on their team who manage the vendor gateway that only the three named vendor staff are allowed through the gateway to access the vendor equipment which URE owns; and
5. Negotiated with the vendor to provide local, dedicated vendor resources for ongoing vendor maintenance and support of these devices, thus implementing more controlled access. At least one dedicated vendor resource has completed URE's security awareness training and provided a PRA, and will thus be allowed access to provide maintenance and support as needed. No other vendor resources will be allowed access until such time as they are compliant with URE security policies and procedures.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016616 CIP-004-3 R3; R3.3 - OVERVIEW

SERC determined that URE failed to document that PRAs for contractor and service vendor personnel with authorized cyber or authorized unescorted physical access to CCAs occurred pursuant to CIP-004-3. The URE PRA program did not have established criteria to evaluate any identified criminal history. Instead, when a PRA produced criminal exceptions, the URE legal department reviewed the PRA on a case-by-case basis.

On some occasions, URE required a completed PRA certification form from the vendor or contractor for individuals assigned to work within the URE CIP environments in situations where the contractor or vendor could not or would not subject the individual to the URE PRA process. The URE PRA certification form asked if there was any adverse information found during the vendor or contractor's PRA, but URE did not establish or provide any criteria for what constituted this criteria. In the event that the contractor or vendor determined that adverse information existed, based on its own criteria, URE would require additional information and details in order to make decisions and document reasons for either proceeding with employment or declining to pursue employment.

URE conducted its extent-of-condition assessment to determine the scope of this violation; 5.1% of the total population of individuals with authorized access to CCAs went through the PRA process where the contractor or vendor company conducted the PRA and provided the certification to URE.

The cause of this violation was a deficient PRA process. URE did not have defined criteria for what constituted acceptable or unacceptable PRA results.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document what constituted acceptable or unacceptable PRA results for a period of at least six years could result in inconsistent assessments of personnel being evaluated for authorized access to CCAs. In the case of some contractors or vendors, URE was wholly dependent on the content and quality of the third-party review and the third kicparty's identification of any adverse information, as defined by the third party. Nevertheless, URE reviewed and assessed PRA results in which a third party identified any adverse information when conducting its own PRA.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Obtained a redacted PRA or performed a PRA for all outside contractors and service vendors with ESP or PSP access;
2. Approved changes to the human resources (HR) onboarding for contractors process to require that, for contractors, URE will either perform the PRA itself through its own provider, or will obtain a redacted PRA from the contracting agency;
3. Completed training on the HR onboarding for contractors process with reading and signing by relevant staff in multiple departments.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016015515 CIP-004-3a R3; R3.2 - OVERVIEW

SERC determined that URE failed to update each PRA at least every seven years after the initial PRA. The URE compliance department received a completed PRA renewal for a contract security guard. Upon review, the compliance department employee discovered that the preceding PRA had expired seven years after the initial PRA was completed, resulting in a gap of 85 days where the contract security guard did not have a valid PRA and retained his or her authorized unescorted physical access rights to CCAs.

The cause of the violation was the URE employee tasked with managing the reports to identify pending PRA expirations at the 60-day mark failed to review the reports required by the URE procedure.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to update a PRA could have allowed an individual with a recent criminal history to retain and use their physical access permissions to tamper with or destroy CCAs, thereby affecting normal operations or the reliability of the BPS. Nevertheless, this violation was limited to a single security guard for 85 days. The security guard was in good standing with URE at the time of the violation, and remained so afterward. URE only uses contract security guards licensed by the state, and a part of that license requires that the state conduct PRAs on licensed individuals every two years.

SERC determined the duration of the violation to be approximately 85 days, from the date URE failed to update a contract security guard's PRA every seven years through when URE received an updated PRA for the contract security guard.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had its vendor and the subject contractor complete updated PRAs. No adverse information was found as a result of the PRAs;
2. Initiated an extent-of-condition review to determine the scope and cause of the failure, and determined that there were no other instances where it failed to update a PRA at least every seven years;
3. Implemented its PRA renewal for contractors procedure, which contains steps that are performed by HR to ensure that a new PRA is obtained prior to the expiration date or access will be terminated;
4. Made additional revisions stating that in all cases possible, URE will perform the PRA for contractors with PSP or ESP access itself, and that a redacted PRA can be accepted from a vendor if approved by URE compliance; and
5. Trained all staff affected by the procedure.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012666 CIP-004-3 R4 - OVERVIEW

SERC determined that URE failed to maintain a list of vendor personnel with authorized cyber access to CCAs or ensure that it properly maintained access lists for the vendor personnel. The SERC audit team discovered that third-party vendor personnel had electronic access to four devices that URE had identified as CCAs. The vendor personnel had electronic access to provide remote support. Nevertheless, URE failed to maintain a list of vendor personnel with access to the CCAs or to ensure that access lists for the vendor personnel with authorized cyber access to the CCAs were properly maintained.

The cause of this violation was URE's inadequate oversight and procedures relating to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to maintain access lists of vendor personnel or ensure that access lists for vendor personnel were properly maintained could result in unauthorized individuals gaining access to and compromising identified CCAs, including the EMS, adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support

agreement with the vendor where the vendor personnel are to undergo stringent vetting, including a criminal background check and identity verification. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE created a list of the approved vendor resources with authorization to access the CCAs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a BES Cyber System access review procedure. This procedure sets forth an access review process conducted by the compliance department, which includes a quarterly process for reviewing vendor support resource access to storage devices;
2. Executed its vendor access procedure;
3. Created a list of named, approved vendor resources who are authorized to provide on-site support on the devices through a shared account that is logged into by URE staff and with a login and password known only to URE staff;
4. Completed a review that its list of individuals with ESP or PSP access is complete and accurate and produced a complete listing of all individuals with access to BES Cyber Systems and an indication of access, as well as a list of shared accounts from the URE domain; and
5. Conducted the following training:
    a. The compliance department staff having responsibility for the contractors access list completed a read-and-sign review of the access list process;
    b. System administration staff completed a read-and-sign review of the vendor access procedure; and
    c. The staff from multiple departments having responsibility for the URE CIP Asset user access procedure completed a read-and-sign review.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015480 CIP-004-3a R4; R4.2 - OVERVIEW

SERC determined that on two occasions URE failed to revoke access to CCAs within seven calendar days for individuals who no longer required such access. URE identified each instance of noncompliance through recently implemented internal controls.

In the first instance, URE terminated a contractor due to the end of the contract obligations, not a for-cause termination. When an HR representative submitted the form to have the contractor's electronic access permissions revoked, he or she misspelled the contractor's last name, and URE eliminated access permissions for the incorrect user ID, which had been previously created as a result of a past request for access that again involved misspelling of the contractor's last name.

In the second instance, promoted an employee to a new role. The employee's manager requested revocation of existing electronic access permissions on the same day. However, due to a failure to create the proper work order within the required seven calendar days, URE did not revoke the electronic access permissions until 23 days after URE promoted the employee to a new role.

The cause of the violation was a human performance failure by URE personnel to follow the established access revocation procedures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to revoke access to CCAs could have allowed individuals to access CCAs without proper authorization and misuse, damage, or destroy CCAs to the detriment of the reliability of the BPS. Both involved individuals were in good standing with URE at the time of the occurrence. URE determined that the individuals had not used or accessed the relevant accounts after they were terminated or changed positions.

SERC determined the duration of the violation to be approximately ten months, from eight days after the contractor was terminated in the first instance of noncompliance through when URE revoked access permissions for the last individual involved in the violation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

First Instance:

1. Removed physical access and deleted the Virtual Machine (VM) used by the contractor to access the ESP. These actions removed access and prevented the user from accessing the ESP and entering any URE facility in order to log on directly to a system;

2. Submitted a domain account removal request to remove the terminated contractor's user account and virtual private network (VPN) access, and the account was removed. No VPN account existed;
3. Implemented URE's revocation process. This process defines the steps that URE follows to ensure that when a termination occurs, all user access is removed. As an additional step to verify that all access has been removed, a compliance analyst is required to verify and ensure that all access has been removed;
4. Trained all URE staff affected by the updated revocation process;
5. Generated new reports from URE's HR management system (HRMS) and IT management system no later than the first business day of the month for a monthly review; and
6. Held a training session related to the monthly CIP-related access reconciliation of the HRMS and IT management system reports for all members of URE's relevant department. This department has responsibility for completing the monthly tasks related to this CIP-related access reconciliation.

Second Instance:

1. Removed the subject employee's access to CCAs and protected Cyber Asset information;
2. Approved revisions to URE's revocation process to take all transferring employees down to a level of access common to all URE employees; and
3. Trained all URE management on the new processes.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016615 CIP-004-6 R5; R5.2 - OVERVIEW

SERC determined that URE failed to remove access to High Impact BES Cyber Systems prior to the end of the next calendar day after the date on which the need to remove access was determined. URE discovered that an employee who transferred to a different department did not have authorized electronic and authorized unescorted physical access permissions to the High Impact BES Cyber Systems and the associated BES Cyber Assets removed by the end of the next calendar day. URE removed the individual's access permissions upon discovery—one day later.

The cause of the violation was that the URE process requires a URE manager to approve all employee transfers. This approval within the Human Resources system triggers the subsequent access revocations. In this instance, the manager approved the workflow a day late, resulting in this violation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to revoke an individual's authorized electronic and authorized unescorted physical access by the end of the next calendar after access was no longer required could have allowed the individual to use his or her access permissions to degrade URE operations or negatively affect the BPS. Nevertheless, URE revoked the access one day after it should have revoked access, limiting the duration of the violation. The single employee at issue was current on cybersecurity training, had a valid PRA, and was in good standing with URE.

SERC determined the duration of the violation to be approximately 12 hours, from the day after authorized electronic and authorized unescorted physical access should have been revoked through when URE removed authorized electronic and authorized unescorted physical access.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Conducted an extent-of-condition assessment, reviewed previous transfers conducted within the past 90 days, and discovered no additional instances of noncompliance;
2. Terminated the remaining access for the employee;
3. Approved revisions to its transfers process requiring a compliance analyst to generate a second access report after access removals have been completed to ensure that all access was removed by the end of the next calendar day following the effective date or transition date for the transfer;
4. Approved revisions to its revocation process to take all transferring employees down to a level of access common to all URE employees; and
5. Trained all URE management on the new processes.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017016813 CIP-004-6 R5; R5.4 - OVERVIEW

SERC determined that URE failed to remove a non-shared user account for access to High Impact BES Cyber Assets for a terminated individual within 30 calendar days of the effective date of the

termination action. A URE employee resigned from URE on good terms to take a new position outside of URE. On the same day, URE took possession of the employee's card access badge and removed the employee's ability to gain physical access, took possession of the employee's laptop, eliminated the employee's domain account and VPN account, and revoked the employee's two-factor authentication access. These actions by URE effectively eliminated the ability of the employee to access any URE system, site, or Cyber Asset.

Approximately two months later, while conducting a quarterly access review, URE discovered that this former employee had an active user account on two BES Cyber Assets. URE did not revoke the employee's local user account on two servers.

The cause of this violation was insufficient training resulting in the human error of failing to delete the terminated individual's user account.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to revoke a terminated individual's user account could allow a malicious individual to access and use it in order to disrupt URE operations or create negative impacts to the BPS. Nevertheless, URE removed the terminated individual's ability to physically access any URE facilities and remotely access any URE systems on the last day of employment. URE's ESPs and the PSPs established by URE would thwart any access attempts by an outsider, and any internal threats by URE personnel would have to know the local user account password.

SERC determined the duration of the violation to be approximately five weeks, from the date 31 days after URE failed to revoke the terminated individual's non-shared user account through when URE revoked the terminated individual's non-shared user account.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Removed the terminated employee's physical access and his domain account;
2. Removed the remaining non-shared user account;
3. Approved a new user account removal procedure which includes all steps that a subject matter expert should use to remove accounts, verify that all accounts have been removed, and attach all evidence to a IT management system ticket;
4. Trained all relevant staff with a read-and-sign of the new user account removal procedure;

5. Improved the overall termination process by combining the involuntary termination and voluntary termination processes which ensure advance notification to staff responsible for removing access for both types of termination in its access termination process; and
6. Trained all staff affected by the updated access revocation terminations process with a read-and-sign of the process.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012667 CIP-005-3 R1; R1.1; R1.5 - OVERVIEW

SERC determined that URE failed to identify and document all access points to the ESP and failed to afford EACM devices all of the protective measures specified in CIP-005 R1.5.

The cause of this violation was URE's decision to configure a corporate firewall outside of the identified ESP that URE operated as if it were an ESP. URE did not identify this outer corporate firewall as an ESP and thus did not include it in its CIP program or provide it with the protections required by the CIP Standards.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to identify all access points to the ESP could result in inadequate protection of the access points and provide an opportunity for malicious individuals to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS. URE's failure to afford EACM devices all of the protections specified in CIP-005 R1.5 could result in vulnerabilities to the ESP going unaddressed and provide an opportunity for malicious individuals to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS.

Several factors increased the risk of the violation. The vendor personnel in URE's CIP-004 violations had electronic access to the devices which URE identified as CCAs, but URE had not ensured that those individuals had completed cybersecurity training or had valid PRAs, and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. URE had no means of ensuring the authenticity of the vendor personnel accessing the devices from outside the ESP, who were able to use a URE shared account to make changes to those devices remotely. Nevertheless, URE provided additional access control on the corporate firewalls which restricted the ports and services that had access to the CIP network. In addition, the vendor personnel whose authenticity were not verified at the ESP access points were operating under a service agreement with the vendor and underwent a background check prior to starting employment with the vendor. The

vendor personnel also had to use an individual username, password, and two-factor authentication token to gain access to the vendor gateway on URE's corporate network before accessing the devices.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

Issue 1: Electronic Access Points (EAPs)

1. Created, to correct the various devices that were incorrectly configured, a number of change requests to move the management consoles' IP addresses inside of the ESP. URE began moving these assets identified as EAP's into the ESP completely (removing any IP addresses outside the ESP). By placing these management interfaces into the ESP, the unidentified EAPs specified in the violation cease to exist;
2. Created an asset management process, including a new asset request process, to address the identification and documentation of BES Cyber Systems and the underlying CIP Assets comprising the BES Cyber Systems;
3. Updated and approved a document with steps to ensure that, for new devices, no ESP IP addresses will exist on a non-ESP asset, and that no non-ESP IP addresses existed on an ESP asset;
4. Implemented a URE CIP Asset classifications procedure, which is URE's process for identifying and correctly classifying URE CIP Assets. The URE CIP Asset classification document combined and replaced URE's BES Cyber Systems categorization process and URE CIP Asset classification procedure;
5. Completed an annual review of all URE assets to ensure not only the proper classification of URE CIP Assets, but also a review of those that are not identified as CIP Assets;
6. Conducted training on the new and revised procedures.

Issue 2: Ports and Services

1. Implemented a ports management process that sets forth the process for adding, updating, and decommissioning ports that have been determined to be needed for URE CIP Assets;

2. Implemented a ports and services database reconciliation procedure that details the procedure the administrator uses for reconciling the data with the ports and services database and conducting a monthly validation;
3. Made updates effective in CIP task templates (for asset new builds, asset changes, and asset decommissions) related to ports and services tasks. Notification of the updates was sent to the IT department email distribution the same day;
4. Completed a review of the listing of all ports in its ports and services database that contains the data for the open logical network accessible ports for all URE CIP Assets and their associated justifications, and the justifications for the ports undergoing testing were further updated to add the IT management system ticket for additional testing to determine if closure is possible;
5. Conducted training and distribution of information related to ensuring that only ports and services required for normal and emergency operations were enabled and proper justification of such ports;

Issue 3: Patch Management

1. Developed the final in-scope Cyber Asset software and patch source list. The patch source list was revised to make clarifications to patch sources and supplemental information;
2. Documented the patch management process in its CIP patch management process pursuant to CIP-007-5 R2;
3. Finalized a review of patch levels to ensure that patches on all URE CIP Assets were at the appropriate patch level;
4. Completed patching cycle;
5. Conducted training related to this violation and the mitigation steps;

Issue 4: Cyber Vulnerability Assessment (CVA)

1. Developed a CVA procedure;
2. Had relevant staff complete a read-and-sign of CVA procedure;
3. Held a kick-off meeting to discuss the upcoming CVA and the roles and responsibilities, with a make-up session, for representatives from relevant teams;
4. Completed its CVA; and

5. Shifted responsibility to conduct the annual CVA from one analyst in the compliance department to the entirety of a certain department to leverage the larger number of personnel and their focus on cybersecurity and thus ensure that the next CVA was conducted on time. URE also created an automated incident ticket to remind the relevant department when it is time to begin the CVA.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016619 CIP-005-3a R1 - OVERVIEW

SERC determined that URE failed to have all External Routable Connectivity go through an identified EAP.

The cause of this violation was a misinterpretation of the CIP Standard language. URE interpreted the CIP Standards and concluded that data traveling across an ESP to another ESP would not be in violation of the CIP Standards. In addition, URE determined that since it managed and routed the network traffic, the mingling of the CIP traffic with corporate traffic was not an issue or a compliance risk.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify and protect EAPs on the mixed trust infrastructure could have left Cyber Assets or BES Cyber Systems vulnerable to denial of service attacks and CIP data vulnerable to theft via attacks on the corporate network. URE's failure to identify and protect EAPs used to communicate between the two data centers could leave CIP data vulnerable to theft. Nevertheless, URE monitored the communication links to the corporate network with intrusion detection and prevention systems to detect and alert on traffic anomalies. URE encrypted all traffic between the two data centers, minimizing the risk that any intercepted data could be used for malicious purposes.

SERC determined the duration of the violation to be ongoing, from the date when URE implemented a mixed trust environment and did not identify the resulting EAPs to the ESPs through when URE is expected to complete its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide a network diagram depicting the ESP network and describing the functions of relevant devices;

2. Provide an update to SERC on the status of any Standard Drafting Team efforts that would allow the continued use of the ESP design in question;
3. Provide a draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design;
4. Complete trenching and laying of private fiber and install the new circuits at the facilities containing the ESPs;
5. Complete testing and move all corporate data traffic off of the mixed trust routers, which will resolve the mixed trust issue;
6. Update its network diagrams to identify any changes to BES Cyber Systems, EAPs, EACMS, PACS, and PCAs resulting from the resolution of the mixed trust issue;
7. Provide an update on the draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design; and
8. If a revised Standard allowing the use of the ESP design is not approved by FERC, URE will submit a revised Mitigation Plan to SERC that will document how and by what date URE will eliminate the ESP design. If the revised Standard is still in process but not yet approved, URE will consult with SERC on appropriate steps forward.

In addition, to mitigate this violation URE:

1. Approved CIP review process to provide required actions in the event that there is a creation or redesign of large-scale solutions related to the ESP;
2. Completed training on the CIP review process with a read-and-sign by relevant staff;
3. Executed a contract with vendor to install new circuits at the facilities containing the ESPs; and
4. Provided an update to SERC on circuit installation status.

Mitigation activities for this violation are still ongoing.

SERC2017017849 CIP-005-3a R1; R1.1 - OVERVIEW

SERC determined that URE failed to identify all access points to the ESP for all externally connected communication end points terminating at any device within the ESP. A user could move from the corporate network to the ESP network without having to authenticate through an ESP access point.

The cause of this violation was inadequate processes for URE to identify and prevent a dual-homed issue, with the resulting failure to identify an ESP access point, from occurring.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify the dual-homed scenario and resulting failure to identify an ESP access point could have allowed a malicious individual to move from the corporate network segment on the corporate side of the dual-homed device to the ESP network unchallenged by an appropriate access point. Nevertheless, the ESP and corporate, non-ESP network segments of these two Cyber Assets resided within a protected network segment, secured by a corporate firewall, which restricted access to a limited number of individuals. URE also utilizes an intrusion detection system with real-time alerting on any anomalous network activity.

SERC determined the duration of the violation to be approximately 18 months, from the date when URE implemented the dual-homed PCAs, thereby creating an ESP access point, through when URE removed the back-up functionality from the ESP interface, thereby removing the ESP access points.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the relevant department implement a control to review all interfaces before the asset is placed into production as part of its pre-production vulnerability assessment;
2. Had all relevant department staff complete training on this interface review control through a read-and-sign;
3. Had the relevant department institute a control performing an additional review of server builds to verify that the asset is not dual-homed and has the right network connection;
4. Had all relevant staff complete training on this server build review control through a read-and-sign; and
5. Completed additional training on acceptable network connectivity for BES Cyber Systems by relevant departments.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012668 CIP-005-3 R2; R2.2; R2.4 - OVERVIEW

SERC determined that URE failed to: (1) enable only the ports and services required for operations and for monitoring Cyber Assets within the ESP; and (2) implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party where external interactive access into the ESP was enabled. URE allowed full-range host-to-host communications to traverse the ESP access points, in effect failing to disable the ports and services not required for operations or monitoring of

Cyber Assets within the ESP. URE vendor personnel remotely connect through the dedicated vendor gateway and must authenticate at the gateway using a vendor username and password, as well as a two-factor authentication token. Nevertheless, when the vendor personnel access the devices, they use a URE shared account that URE personnel also use. URE does not verify the authenticity of the vendor personnel accessing the devices within the ESP at the access point as required by CIP-005 R2.4.

The cause of this violation was a lack of organizational processes and technical and procedural mechanisms for control of electronic access at all EAPs to the ESP.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to enable only those ports and services at the ESP access points that were required for operations and for monitoring Cyber Assets within the ESP increased the risk of unauthorized access though ports that were unnecessarily left enabled. Furthermore, URE's failure to verify the authenticity of the individuals accessing the devices at the ESP access points increased the risk of unauthorized access to CCAs. These failures could result in the compromise of CCAs, thereby reducing or eliminating URE's situational awareness over its portion of the BPS. The vendor personnel in URE's CIP-004 violations had electronic access to the devices, but URE had not ensured that those individuals had completed cybersecurity training or had valid PRAs, and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. Nevertheless, URE provided additional access control on the corporate firewalls which restricted the ports and services that had access to the CIP network. In addition, the vendor personnel whose authenticity were not verified at the ESP access points were operating under a service agreement with the vendor and underwent a background check prior to starting employment with the vendor. The vendor personnel also had to use an individual username, password, and two-factor authentication token to gain access to the vendor gateway on URE's corporate network before accessing the devices.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Moved all relevant firewall rules from the corporate firewalls to the ESP firewalls, and the "default allow" status was changed to a "default deny" status on the ESP firewalls;
2. Reviewed the justifications of firewalls and initiated removal for any firewall access no longer needed;
3. Updated the network ESP technical documentation process to require that URE will use a "deny by default" rule and enable only needed ports and services when commissioning new firewalls.

Also updated the firewall deny by default procedure to detail how the "deny by default" requirement is implemented as firewalls are operated and managed;

4. Transferred management consoles from the corporate environment into the ESP, and the management console was readdressed so that all interfaces reside inside an ESP and no interfaces exist outside of an ESP;
5. Purchased and installed dedicated new hardware for use in the ESP;
6. Notified affected staff via email of the technicians allowed on-site to work on the consoles pending the completion of URE on-boarding requirements;
7. Changed the access on the gateway within the ESP to "Deny All", closing the gateway portal and removing the ability for technicians to access the gateway remotely;
8. Executed a storage administration vendor access procedure, which includes the required actions for maintenance and upgrades and specifically requires that they come on-site and be escorted by URE personnel;
9. Created a list of contractors with access to ESP storage to centralize the list of named, approved vendor resources who are authorized to provide on-site support on the consoles through a shared account that is logged into by URE staff and with a login and password known only to URE staff;
10. Updated URE policies and procedures so that the ESP network can only be logically accessed via the interactive access layer; and
11. Completed departmental read-and-sign training for all relevant staff.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016620 CIP-005-3a R2; R2.2 - OVERVIEW

URE did not, at all access points to the ESP, enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, and did not document the configuration of those ports and services. SERC determined that URE failed to require inbound and outbound access permissions at all EAPs for High Impact BES Cyber Systems and deny all other access by default.

The cause of this violation was a failure by URE staff to understand the operational risks and compliance impacts when reconfiguring ESPs.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to restrict ports and services on EAPs on the mixed trust infrastructure could have left BES Cyber Assets and BES Cyber Systems vulnerable to denial of service attacks and CIP data vulnerable to theft via attacks on the corporate network. URE's failure to restrict ports and services on EAPs used to communicate between the two ESPs could leave CIP data vulnerable to theft. Nevertheless, URE monitored the communication links to the corporate network with intrusion detection and prevention systems to detect and alert on traffic anomalies. URE encrypted all traffic between the two ESPs, minimizing the risk that any intercepted data could be used for malicious purposes.

SERC determined the duration of the violation to be approximately five years, from when URE implemented a mixed trust environment and did not enable only those ports and services required for operations and for monitoring Cyber Assets within the ESP on the resulting ESP access points without documenting the configuration of those ports and services, through when URE is expected to complete its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide a network diagram depicting the ESP network and describing the functions of relevant devices;
2. Provide an update to SERC on the status of any Standard Drafting Team efforts that would allow the continued use of the ESP design in question;
3. Provide a draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design;
4. Complete trenching and laying of private fiber and install the new circuits at the facilities containing the ESPs;
5. Complete testing and move all corporate data traffic off of the mixed trust routers, which will resolve the mixed trust issue;
6. Update its network diagrams to identify any changes to BES Cyber Systems, EAPs, EACMS, PACS, and PCAs resulting from the resolution of the mixed trust issue;
7. Provide an update on the draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design; and
8. If a revised Standard allowing the use of the ESP design is not approved by FERC, URE will submit a revised Mitigation Plan to SERC that will document how and by what date URE will

eliminate the ESP design. If the revised Standard is still in process but not yet approved, URE will consult with SERC on appropriate steps forward.

In addition, to mitigate this violation URE:

1. Approved a CIP review process to provide required actions in the event that there is a creation or redesign of large-scale solutions related to the ESP;
2. Completed training on the CIP review process with a read-and-sign by relevant staff;
3. Executed a contract with vendor to install new circuits at the facilities containing the ESPs; and
4. Provided an update to SERC on circuit installation status.

Mitigation activities for this violation are still ongoing.

SERC2013012669 CIP-005-3 R4; R4.2; R4.3; R4.4 - OVERVIEW

SERC determined that URE failed to perform an annual CVA on the access points to the ESP that: (1) disabled all ports and services that were not required for normal or emergency operations; (2) included the discovery of all ESP access points; and (3) provided documented evidence that a review of controls for default accounts, passwords, and network management community strings was completed.

The cause of this violation was URE did not have adequate documentation procedures relevant to the CVA.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to perform the annual CVA in accordance with the requirements of CIP-005 R4 could leave ESP access points in an insecure state, providing malicious individuals an opportunity to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS. Nevertheless, URE subject matter experts reviewed the CVA results in order to confirm whether specific ports or services were required to be enabled, which could help identify any enabled ports and services that should be disabled. URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately six-and-a-half years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed a CVA procedure;
2. Had relevant personnel complete a read-and-sign of the CVA procedure;
3. Held a meeting to discuss the roles and responsibilities for an upcoming CVA;
4. Completed a CVA; and
5. Shifted responsibility of the CVA to ensure it is conducted on time.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012670 CIP-005-3 R5; R5.1; R5.2 - OVERVIEW

SERC determined that URE failed to ensure that all documentation required by CIP-005 reflected current configurations and processes as required by CIP-005 R5.1. SERC also determined that URE failed to update documentation required to support compliance with the requirements of CIP-005 within 90 calendar days of making modifications to the network or controls as required by CIP-005 R5.2.

The cause of this violation was URE's lack of a documented process to ensure compliance with the Standard, which allowed for human error and procedural breakdown.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that all documentation required by CIP-005 reflected current configurations and processes as required by CIP-005 R5.1 and to demonstrate that it reviewed all documentation and procedures required by CIP-005 at least annually could result in incomplete or inaccurate documentation of the ESP and associated Cyber Assets, which could lead personnel to take incorrect actions based on outdated or missing information. URE's failure to update documentation to reflect network changes within 90 days of the change as required by CIP-005 R5.2 could result in the misrepresentation of the network and ESP, which could result in misidentification of the Cyber Assets necessary for URE's situational awareness of the BPS and possibly impede or delay URE's ability to respond to or recover from an emergency. Furthermore, inaccurate drawings of the ESP and associated Cyber Assets could result in a failure by URE to identify all Cyber Assets within the ESP, including Cyber Assets that were introduced without authorization, and all access points to the ESP, which could provide unauthorized access to CCAs and other Cyber Assets.

Nevertheless, URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of

unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately five-and-a-half years, from the date the audit period began through when URE updated its network diagrams.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Added revision history and cover sheet to the network diagram documenting the changes made to the network diagram and the dates those changes were made. In addition, URE began annually approving the network diagram;
2. Implemented a network ESP technical documentation process for documenting the ESP to include the network diagram, external routable communication paths, and inbound and outbound ESP access point rules;
3. Updated URE's change management process to include task templates used whenever a change impacted a CIP asset to update any CIP-related documentation that may have changed as part of that change request work, ensuring that any documentation gets reviewed and updated as part of the change request; and
4. Provided training related to this violation and mitigation on the network ESP technical documentation process and had a departmental read-and-sign.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015523 CIP-005-3a R5; R5.1 - OVERVIEW

SERC determined that URE failed to review at least nine documents in one annual CIP documentation review. URE discovered this violation while preparing for the implementation of CIP Version 5.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure it conducted the annual review, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct an annual review of its CIP-005-3 documents and procedures could have resulted in outdated configurations, documents, procedures, and processes around its ESPs and electronic access controls remaining in effect, possibly introducing gaps in the protections provided by the ESPs and electronic access controls. The risk of this violation was elevated

by similar URE failures to annually review documentation in NERC Violation IDs SERC2016015522 (CIP-002-3 R4), SERC2016015524 (CIP-006-3 R1.8), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and compliance with the CIP Standards. Nevertheless, this violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from the date URE failed to annually review the documents and procedures referenced in CIP-005-3 through when URE completed the annual review of its documentation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved the documentation required in CIP-005 R1, R2, and R3;
2. Created a department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP program; and
3. Built a document management database that tracks review dates and will trigger reviews and updates for business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012671 CIP-006-3a R1; R1.2; R1.8 - OVERVIEW

SERC determined that URE failed to: (1) identify all physical access points through each PSP; and (2) ensure the senior manager or delegate reviewed and approved its physical security plan annually.

The cause of this violation was inadequate processes and procedures.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify physical access points to the PSP could leave those physical access points without appropriate protections against unauthorized physical access. This could allow unauthorized individuals to gain physical access to CCAs, giving them the ability to damage, destroy, or misuse the CCAs, thereby reducing or eliminating URE's situational awareness of the BPS. In addition, URE's failure to have the senior manager or delegate approve the physical security plan and its failure to annually review the physical security plan could result in changes to the PSP going undocumented and indicates a weakness in URE's internal controls leading to an inconsistency in the

application of its CIP program, which could result in weaknesses in the physical protection of Critical Assets and CCAs.

Nevertheless, at the first location URE had deployed a card reader, door contact, and an exterior camera to protect against unauthorized access and log entry at the access point. At the second location, the first access point did not have a camera monitoring it but could only be opened from the inside and would alarm to a centralized alarm monitoring station upon opening. The second access point had a door contact that would alarm when opened and an interior camera for monitoring, while the third access point had a magnetic lock, card reader, and an exterior camera deployed. In addition, the physical security plan was reviewed by a specific manager in two prior consecutive years, indicating that URE personnel were aware of the need to review the physical security plan annually. The PSPs in question were also protected by fences and locked gates, limiting the ability of unauthorized individuals to gain physical access to the PSPs.

SERC determined the duration of the violation to be approximately 5 years and 11 months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Added the PSP access points identified as missing to URE's physical security plan, which was approved by the CIP senior manager;
2. Added a PSP access point section to the physical security maintenance and testing procedure, requiring performance of a visual inspection of the entire PSP to look for changes related to physical access points;
3. Improved the visual inspection process outlined in the physical security maintenance and testing procedure with a revision to the physical security inspection forms; and
4. Provided training on the physical security maintenance and testing procedure to the relevant team members with job functions related to the access point visual inspection and had those individuals complete a read-and-sign acknowledgement.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015516 CIP-006-3c R1; R1.6 - OVERVIEW

SERC determined that URE, in over 1,900 instances, failed to implement its visitor control program for visitors without authorized unescorted access to a PSP.

The cause of this violation was URE's failure to exercise sufficient oversight and conduct sufficient training to ensure adequate implementation of the URE visitor control program. URE failed to follow its visitor control program in a variety of ways, including failures to include visitor names or legible visitor names within the logbooks, failures to document the time that visitors entered and exited the PSP, and failures to document the identity of the escort for visitors within the PSP.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to implement its visitor control program on over 1,900 occasions could have allowed unauthorized personnel to gain physical access to CCAs and manipulate, disable, or destroy them to the detriment of the reliability of the BPS. Nevertheless, the PSPs in question are staffed with operations staff as well as security 24 hours a day, seven days a week and have closed circuit television feeds to the security console.

SERC determined the duration of the violation to be approximately two-and-a-half years, from the date of the earliest noted issue found by URE during its extent-of-condition review through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Dismissed the contracted security guard that failed to properly escort a visitor from working at URE;
2. Conducted a refresher escort training for all contracted security guards;
3. Delivered the updated URE training to all contracted security guards which included procedures for escorting non-authorized persons into the PSP;
4. Issued an order to all contract security guards, directing the proper procedure for logging visitors' entry and exit from certain parts of the PSP;
5. Issued an order to all contract security guards, directing the proper procedure for logging visitor's entry and exit from certain parts of the PSP other than the previous order; and
6. Implemented a new procedure for gathering and reviewing the visitor log book.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015524 CIP-006-3c R1; R1.8 - OVERVIEW

SERC determined that URE failed to implement its physical security plan's requirement to perform an annual review of its physical security plan. URE discovered this violation while preparing for the implementation of CIP Version 5.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual review, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct an annual review of the physical security plan could have resulted in outdated documentation of its PSPs and physical access controls, possibly introducing gaps in the protections provided by the PSPs and physical access controls. The risk of this violation was elevated by similar URE failures to annually review documentation in NERC Violation IDs SERC2016015522 (CIP-002-3 R4), SERC2016015523 (CIP-005-3 R5), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and compliance with the CIP Standards. Nevertheless, this violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately one month, from one day after URE failed to implement its physical security plan's requirement to annually review the physical security plan through when URE completed its annual review of the physical security plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved URE's physical security plan;
2. Created a department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP Program; and
3. Built a document management database that tracks review dates and will trigger reviews and updates for business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016603 CIP-006-6 R1; R1.3 - OVERVIEW

SERC determined that URE failed to utilize two different physical access controls to allow authorized individuals to have unescorted physical access into PSPs protecting High Impact BES Cyber Systems and

their associated EACMS and PCAs. Shared knowledge of a personal identification number (PIN) between the authorized individual and a system administrator rendered this physical access control insecure. URE determined that one of the two separate physical access controls it utilized to allow authorized unescorted physical access into relevant PSPs was not secure. The two physical access controls URE utilized were (1) a coded badge that an authorized individual possessed and (2) a personal identification number code that an authorized individual knew. However, when URE authorized unescorted physical access to an individual, one of two URE system administrators for the Physical Access Control System entered the PIN code that the authorized individual selected into the PACS. As a result, a system administrator knew the PIN code for any individual that he or she authorized to have unescorted physical access to the relevant PSP. The shared knowledge of each such PIN code between the authorized individual and a system administrator rendered this physical access control insecure.

The cause of this violation was a lack of understanding around this specific requirement and the need for the PIN to be secure to each individual authorized for unescorted physical access to the PSPs in question. URE's procedures did not ensure that each authorized individual entered their unique PIN into the PACS to avoid shared knowledge of the PIN.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that each authorized individual was the only person that knew their PIN code could have allowed an individual to obtain an authorized individual's badge and use the PIN code to gain unauthorized physical access to PSPs protecting High Impact BES Cyber Systems and take action to negatively impact the reliability of the BPS. Reducing the risk, only two URE system administrators entered the PIN codes for authorized individuals into the PACS, and both system administrators had authorized unescorted physical access to all URE PSPs. URE operators and control staff are present in PSPs 24 hours a day, 7 days a week, limiting the ability of an unauthorized individual to enter a PSP without being noticed. URE maintains on-site armed security staff that could be notified if an unauthorized individual was observed entering or exiting a PSP. URE security staff also monitors multiple camera feeds from all PSP access doors, allowing identification of any unauthorized individual.

SERC determined the duration of the violation to be approximately six months, from the date the standard became mandatory and enforceable through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Executed a physical access user management process to require that when receiving card key badges permitting access into a PSP, that the PIN must be entered by the individual receiving the badge;
2. Completed training for applicable staff with a read-and-sign of the physical access user management process;
3. Installed a separate key pad, which allows the individual receiving the badge to securely enter his or her PIN into the keypad, which is separate from the keyboard the administrator uses to create the badge; and
4. Conducted PSP obligations and responsibilities training, which included training on PIN creation and confidentiality for badge holders who have unescorted access into a PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012678 CIP-006-3a R2 - OVERVIEW

SERC determined that URE failed to afford all of the protective measures specified in CIP-007 R2 and R3 to Cyber Assets used to authorize access to the PSP or PACS devices. URE's process for ensuring that only those ports and services required for normal and emergency operations was documented but did not describe how to do this for PACS devices. Although URE reviewed the enabled and disabled ports and services on PACS devices, it did not document the resulting list of ports and services or the justification for why a specific port or service should be enabled or disabled. Without a documented list of the required ports and services for the PACS devices, URE relied on its subject matter experts to review the enabled ports and services based on their expertise, leaving room for subjective decisions and human error.

The SERC audit team also found that URE failed to afford the protective measures specified in CIP-007 R3 to the PACS devices. URE's security patch management program was documented but did not address the need for tracking, evaluating, testing, and installing applicable cybersecurity patches on PACS devices. In addition, URE did not assess some cybersecurity patches or upgrades for PACS devices within 30 days of the availability of the security patches or upgrades. A contributing factor to this failure was the fact that URE did not maintain a documented inventory of the third-party applications installed on PACS devices, making it difficult for URE to ensure that it tracked the availability of security patches and upgrades for each third-party application.

The cause of this violation was that URE lacked adequate procedures to document that it afforded the protective measures as specified by CIP-007 R2 and R3 to the PACS devices.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failures to describe in its procedures how to ensure that only the ports and services required for normal and emergency operations were enabled, to document the need for the assessment of security patches and upgrades for PACS devices, and to assess security patches and updates within 30 days of availability increased the risk of unauthorized electronic access to PACS devices through ports that should have been disabled or through vulnerabilities that were addressed in security patches or upgrades. A malicious individual with unauthorized electronic access to PACS devices could tamper with or disable the PACS devices, allowing unauthorized physical access to CCAs protected within the PSPs. Nevertheless, the PSPs in question were protected by fences and locked gates, limiting the ability of unauthorized individuals to gain physical access to the CCAs and other Cyber Assets within the PSPs.

SERC determined the duration of the violation to be approximately six years and two months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Moved, with the implementation of a CIP patch management process, all physical access controls under URE's standard process, which includes the process for evaluating, testing, and installing applicable security patches on all URE CIP Assets, including the physical access controls;
2. Maintained an inventory of software installed on CIP assets as part of its in-scope Cyber Asset software and patch source list;
3. Included all PACS devices in a patching cycle;
4. Finalized a process to bring the PACS devices into compliance with CIP-007-6 R1 and R2;
5. Addressed physical access controls under the ports management process and the ports and services justifications were updated for all PACS; and
6. Conducted IT cybersecurity patching training.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016606 CIP-006-6 R2; R2.1 - OVERVIEW

SERC determined that URE failed to maintain continuous visitor escort for one of seven visitors in a group within a PSP protecting High Impact BES Cyber Systems and their associated EACMS and PCAs. During a tour, the escort discovered that one visitor was missing from the tour group. The escort immediately retraced the tour path, and found the missing visitor at the security desk in the foyer, just outside the PSP entrance. The missing individual left the group in order to take a phone call.

The cause of this violation was inadequate training leading to a human performance failure by the URE employee to escort visitors continuously while within the PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to maintain continuous escort of a visitor within a PSP could allow the visitor to physically access High Impact BES Cyber Systems and take action to negatively affect the reliability of the BPS. In this case, URE estimates that the time between the last known contact and the exit from the PSP was no more than five minutes. URE staff and armed security guards are within the building containing the PSP in question 24 hours a day, 7 days a week. URE documented the visitor's entry and exit from the PSP on the URE visitor logbook. All individuals on the tour were industry professionals from a compliance working group, and the visitor at issue was an employee at another entity. The visitor at issue abruptly exited the PSP and stood by the security guard station in the foyer until the rest of the tour group arrived in order to take a phone call.

URE conducted an extent-of-condition evaluation by reviewing the visitor logs and assessing the attendees and the assigned escort of all 41 tours conducted at its PSPs over the preceding quarter. URE then interviewed the escorts for all tours and confirmed via email response that at no point in any of the tours did any visitors leave the group or become unescorted.

SERC determined the duration of the violation to be approximately five minutes, from the time the visitor left the escorted tour group through when the URE escort found the visitor.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the escort locate the visitor and the visitor ultimately exited URE's PSP; and
2. Implemented a new training module that focuses on the obligations of those who have PSP access and what their obligations are respective to escorting visitors inside a PSP at URE.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016611 CIP-006-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to log entry and exit of a visitor to a PSP protecting High Impact BES Cyber Systems in five separate instances. URE initially identified this violation when the URE site manager was reviewing and reconciling visitor logs as a compliance check and discovered a single instance. URE identified the remaining four instances as part of an extent-of-condition evaluation conducted in response to a SERC request for information.

The cause of this violation was inadequate training leading to a human performance failure by URE escorts to follow the URE visitor control process for PSP access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document visitors into a nested PSP could make any forensic investigations following an incident difficult, because records of who was inside the interior nested PSP at any one time would not be readily available and accurate. Nevertheless, the interior PSP was within an access-controlled PSP, so the logs at the exterior PSP were complete, allowing identification of possible visitors to the interior PSP. In addition, URE operators and support staff work within the PSP at all times, allowing identification of visitors who may have entered the interior PSP. URE also maintains on-site armed security staff who work in the facility that contains both the exterior and interior PSPs, and the security staff are located at the front desk sign-in area and make periodic security rounds.

SERC determined the duration of the violation to be five different instances lasting between one minute and approximately one-and-a-half hours, from when URE escorted a visitor into the PSP without completely filling in the manual visitor logbook through when the escorted visitor exited the PSP.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Sent an email message to IT staff reminding them about the rules for documenting escorted visitor access to one of the interior (nested) PSPs;
2. Had a certain URE department implement a new visitor log book review procedure that requires a weekly review of visitor log books to examine the logbook entries for completeness and accuracy and to quickly detect any further violations of the requirement;
3. Completed training for the relevant URE staff responsible for reviewing the visitor log books with a read-and-sign of the visitor log book review procedure; and

4. Implemented a new training module that focuses on the obligations of those who have PSP access and what their obligations are respective to escorting visitors inside a PSP and logging visitor access to a PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017812 CIP-006-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to log entry and exit of a visitor to a PSP protecting High Impact BES Cyber Systems in two separate instances. URE conducted an extent-of-condition evaluation by comparing the prior 30 days of interior PSP logbooks to the exterior visitor logbooks. URE found no additional instances of noncompliance.

The cause of this violation was inadequate training leading to a failure of the escort to follow documented procedures around visitor escorting and interior PSPs nested within another PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document visitors into interior nested PSPs would make any forensic investigations or reviews following an incident difficult, since records of who was inside the interior nested PSP would not exist. Nevertheless, the nested PSPs are within an access-controlled PSP, and the logs at the exterior PSPs were complete. URE operators and support staff work within the exterior PSP at all times. URE also maintains on-site armed security staff who work at the front desk sign-in area and make periodic security rounds.

SERC determined the duration of the violation to be on two occasions, one lasting approximately three hours, and the other lasting approximately 19 minutes, from when the visitor entered the exterior PSP and subsequently advanced to the interior PSP without logging entry in the visitor logbook for the interior PSP through when the visitor exited the exterior PSP without logging the exit from the interior PSP.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Create a new post order for security staff to verbally instruct escorts of the requirement to log all visitor(s) into an interior PSP logbook whenever they are identified in the exterior PSP logbook as having a destination of an interior PSP;

2. Retrain necessary URE staff and security staff on the process of logging all visitors into and out of an interior PSP;
3. Update the weekly visitor log book review to add additional steps; and
4. Train relevant staff on the weekly visitor log book review.

In addition, to mitigate this violation, URE:

1. Confirmed via its records that the first visitor exited the exterior PSP;
2. Confirmed via its records that the second visitor exited the exterior PSP; and
3. Attached new signage at eye level to the front of each interior PSP access point door reminding escorts of the requirement to log visitors into an interior PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012681 CIP-007-3a R2; R2.1; R2.2; R2.3 - OVERVIEW

SERC determined that URE failed to establish, document, and implement a process to ensure that it enabled only those ports and services required for normal and emergency operations and did not submit a request for a Technical Feasibility Exception (TFE).

The cause of this violation was that URE did not have a documented listing of ports and related justifications or a documented process. In addition, URE failed to submit requests for any needed TFEs.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to enable only the ports and services required for normal and emergency operations and its failure to document how to do so for all classes of Cyber Assets deployed within the ESP increased the risk of unauthorized electronic access to CCAs and other Cyber Assets within the ESP through ports and services that should have been disabled. A malicious individual with unauthorized electronic access to CCAs and other Cyber Assets within the ESP could tamper with or disable those devices, including those in the EMS, thereby disrupting URE's situational awareness of the BPS. In addition, URE's failure to document compensating measures or file a TFE for the Cyber Assets on which it was not technically feasible to disable unused ports and services could lead URE to overlook the ability to deploy newly developed compensating measures or new Cyber Assets that were capable of having unused ports and services disabled. Nevertheless, URE had a network-based

intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years and two months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a ports management process, which sets forth the process for adding, updating, and decommissioning ports that have been determined to be needed for URE CIP Assets;
2. Implemented a ports and services database reconciliation procedure that details the procedure the administrator uses for reconciling the data with the ports and services database and conducting a monthly validation. This procedure describes the process for enabling only those logical network accessible ports that are determined as needed through an asset's lifecycle;
3. Made updates effective in the CIP task templates (for asset new builds, asset changes, and asset decommissions) related to ports and services tasks;
4. Completed a review of the listing of all ports in its ports and services database, which contains the data for the open logical network accessible ports for all URE CIP Assets and their associated justifications, and further updated the justifications for the ports undergoing testing to determine if closure is possible; and
5. Conducted training and distribution of information related to ensuring that only ports and services required for normal and emergency operations were enabled and proper justification of such ports.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012675 CIP-007-3a R3; R3.1; R3.2 - OVERVIEW

SERC determined that URE failed to implement a security patch management program for tracking, evaluating, testing, and installing cybersecurity software patches for all Cyber Assets within the ESP. URE failed to document the assessment of security patches and security upgrades for third-party applications deployed on Cyber Assets within the ESP within 30 calendar days of the availability of such patches and upgrades.

The cause of this violation was a lack of adequate process documentation.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to assess security patches and updates within 30 calendar days of availability, and its subsequent failure to implement such security patches and updates or document compensating measures to mitigate risk exposure, left software on the affected CCAs and other Cyber Assets within the ESP vulnerable for an extended period, increasing the risk that a malicious individual could exploit known vulnerabilities that were addressed in security patches or upgrades. In addition, URE's failure to track, evaluate, test, and install applicable security patches and upgrades for third-party applications deployed on the CCAs and other Cyber Assets, and its failure to document compensating measures where it did not install such security patches or upgrades, could lead to vulnerable software going undetected, further increasing the time that a malicious individual could exploit known vulnerabilities. Nevertheless, URE had a network-based intrusion protection system, a host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed the final in-scope Cyber Asset software and patch source list;
2. Documented the patch management process in URE's CIP patch management process pursuant to CIP-007-5 R2;
3. Finalized a review of patch levels to ensure that patches on all URE CIP Assets were at the appropriate patch level;
4. Completed the patching cycle; and
5. Conducted training related to this violation and the mitigation steps.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012676 CIP-007-3a R4; R4.1 - OVERVIEW

SERC determined that URE failed to document compensating measures to mitigate risk exposure for Cyber Assets within the ESP on which URE could not deploy anti-virus and malware prevention tools. The violation involved 12% of the total Cyber Assets and CCAs deployed within its ESPs that were purpose-built devices and were incapable of locally installing anti-virus and malware prevention tools.

The cause of this violation was inadequate process.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document compensating measures or file a TFE for the Cyber Assets for which it was technically infeasible to install anti-virus software and malware prevention tools could lead URE to overlook the ability to deploy newly developed compensating measures or new Cyber Assets that were capable of installing such tools. Nevertheless, the Cyber Assets at issue were deployed within URE's ESP and were protected with an existing network-based intrusion protection system and host-based intrusion detection systems installed on other Cyber Assets within the ESP, and security information and event management tools that could alert URE in the event of unusual activity. These compensating measures, although not documented by URE in a TFE, significantly reduced the likelihood of a malware or virus infection on the Cyber Assets in question and would identify and limit the spread of such an infection on the ESP network.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a response process that sets forth URE's process of an overall defense-in-depth approach for mitigating malicious code under Version 5 of the CIP Standards. This process is consistent with the requirements of CIP Version 5, which does not require TFEs to be filed for devices not capable of supporting antivirus;
2. Approved the response process, which incorporated a requirement that, on a quarterly basis, each team perform a reconciliation against the asset database to ensure that all assets are being protected. Two IT teams are responsible for conducting a quarterly reconciliation; and
3. Conducted training on the revision to response process, which was accomplished with a read-and-sign.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012677 CIP-007-3a R5; R5.1.2; R5.3 - OVERVIEW

SERC determined that URE failed to: (1) implement the required password length, complexity, and annual change requirements as required by R5.3; and (2) document and implement a process to

capture user activity logs to create a sufficient audit trail of user account access activity as required by R5.1.2.

The cause of this violation was insufficient procedures.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Only a single Cyber Asset was technically unable to enforce the password length requirement, and only a few user accounts were not changed annually and were in an expired state that would require an immediate password change had they been accessed. In addition, URE had security systems in place that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. implemented a system access control process;
2. Implemented a security event monitoring process; and
3. Trained relevant personnel on the system access control process and security event monitoring process.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012680 CIP-007-3a R6; R6.1 - OVERVIEW

SERC determined that URE failed to show evidence of security status monitoring for all Cyber Assets within the ESP. URE documented the process to manage its automated security event management program implemented for Cyber Assets within the ESP, but the document failed to include the organizational process controls for Cyber Assets incapable of automated logging.

The cause of the violation was the lack of a process to configure, collect, monitor, and review all assets for security-related events and not submitting TFEs as appropriate.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation involved one Cyber Asset. URE performed an assessment of the Cyber Assets within the ESP and found that this was the only Cyber Asset incapable of having an automated tool

monitor system events related to cybersecurity. Additionally, URE had security systems that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a security event monitoring process;
2. Reconciled, pursuant to its security event monitoring process, the list of assets being monitored against URE's CIP Asset List;
3. Added a task for configuring security event logging and alerting; and
4. Had certain personnel read and sign the security event monitoring process.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012679 CIP-007-3a R8; R8.2; R8.3 - OVERVIEW

SERC determined that URE failed to: (1) perform a review to verify that it enabled only ports and services required for operation of the Cyber Assets within the ESP; and (2) perform a review of controls for default accounts.

The cause of the violation was insufficient processes. URE's annual CVA of all Cyber Assets within the ESP did not adequately verify that only ports and services required for operations of the Cyber Assets within the ESP were enabled and did not demonstrate that it had conducted a review of controls for default accounts.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Nevertheless, URE had security measures in place that could alert URE in the event of unusual activity. Additionally URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed a CVA procedure;
2. Had relevant personnel complete a read-and-sign of the CVA procedure;
3. Held a meeting to discuss the roles and responsibilities for an upcoming CVA;
4. Completed a CVA; and
5. Shifted responsibility for the CVA to ensure it is conducted on time.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015525 CIP-007-3a R9 - OVERVIEW

SERC determined that URE failed to review and update the documentation specified in Standard CIP-007-3a annually. URE depended on individuals within its compliance organization to be aware of the required annual CIP documentation reviews and start the process of preparing for and coordinating the annual review of documentation.

The cause of the violation was a lack of a documented process or controls to ensure the review and approval of documents in a timely fashion.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. This violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from one day after URE failed to annually review and update the documentation specified in CIP-007-3a through when URE completed its annual review and updated the documentation specified in CIP-007-3a.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved documents that were due as required in CIP-007 R1-R7;
2. Created a department to manage process documentation and support quality control for URE's CIP Program; and
3. Built a document management database to track review dates and send notifications.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2017017851 CIP-007-6 R2; R2.1 - OVERVIEW

SERC determined that URE failed to identify itself as the patch source for custom-built software in its patch management process. URE identified multiple custom-built software applications installed on four URE BES Cyber Assets for which URE did not identify itself as the patching source.

The cause of the issue was inadequate procedures for identification of all patch sources.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE issued no security patches for these software applications since deployment. This violation affected only a few BES Cyber Assets and some internally developed software applications. URE utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP.

SERC determined the duration of the violation to be approximately eight months, from the date when the Standard became mandatory and enforceable, through when URE documented itself as the patch source for the custom-built software applications.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide an update to SERC on the status of its extent-of-condition review;
2. Complete an extent-of-condition review
3. Add software applications to URE's patch source list;
4. Complete patch assessments for the developed software applications;
5. Publish its patch management and vendor patch evaluations procedures;
6. Have relevant operations support staff complete training of the patch management and vendor patch evaluations procedure;
7. Update its CIP patch management process; and
8. Create email notifications of the CIP Patch management process.

Mitigation activities for this violation are still ongoing.

SERC2016016614 CIP-007-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to assess patches at least once every 35 days for applicability. The URE employee who had conducted the prior reviews of applicable security patches had accessed the vendor's website but navigated to the wrong page within the vendor website and thus did not find the patches.

The cause of this violation was inadequate training and procedures leading to human error. The URE employee responsible in two prior assessment periods did not go to the correct area of the vendor site to look for available patches.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The affected Cyber Assets were PCAs, and not BES Cyber Assets that were part of one of the High Impact BES Cyber Systems. Neither of the patches were cybersecurity-related. URE maintains a secured ESP within an established PSP.

SERC determined the duration of the violation to be approximately two weeks, from the date when URE had not evaluated the applicability of released patches from its identified patching sources within 35 days through when URE assessed the missed patches.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Evaluated all outstanding patch releases;
2. Had the applicable team sign up for automatic notifications of patches;
3. Approved revisions to the monthly patch verification procedure; and
4. Had specific departments complete training on the monthly patch management verification procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016609 CIP-007-6 R2; R2.3 - OVERVIEW

SERC determined that URE failed to apply applicable patches to 19 servers or create a dated Mitigation Plan within 35 days of the assessment date.

The cause of this violation was inadequate training and procedures leading to human error. The patching owner failed to follow the documented process and apply the patches or create a dated Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In two instances, URE decommissioned an impacted Cyber Asset or removed impacted software to mitigate identified vulnerabilities. In addition, URE had disabled the software prior to its late removal. In total, the violation impacted approximately three percent of URE BES Cyber Assets. URE protected the Cyber Assets at issue within establish ESPs and PSPs, both with real-time monitoring and alerting. URE monitors for any changes to Cyber Asset configurations, and any unapproved changes generate immediate alerts. URE experienced no cybersecurity Incidents during the violation.

SERC determined the duration of the violation to be approximately two months, from the date the when URE exceeded 35 days between the assessment of security patches without applying the applicable patches or creating a dated Mitigation Plan through when URE decommissioned the BES Cyber Asset.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Applied the patches to the relevant servers;
2. Removed a server from the ESP network;
3. Uninstalled system management software;
4. Demonstrated the patching process has been correctly followed;
5. Added personnel to the server administration department;
6. Updated the CIP patch management process;
7. Conducted training related to updates to the patch management process;
8. Approved revisions to the monthly patch verification procedure; and
9. Trained multiple departments on the monthly patch verification procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017811 CIP-007-6 R2; R2.4 - OVERVIEW

SERC determined that URE failed to obtain the approval of the CIP senior manager or delegate to extend the completion date of a mitigation plan created pursuant to CIP-007-6 R2.3 before the timeframe for the original mitigation expired.

The cause of the violation was a failure to implement appropriate internal controls to ensure URE completed mitigation plans by the due date or obtained CIP senior manager (or delegate) approval of extensions to mitigation plan completion dates if required.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement a security patch mitigation plan impacting approximately 14% of the total URE Cyber Assets within the approved timeframe or obtain approval for an extension of the mitigation plan could have resulted in URE overlooking the implementation of the security patch, allowing a security vulnerability to remain on its systems for an extended period. Nevertheless, the actions URE put in place to mitigate the vulnerabilities addressed by the security patch have remained in place since the mitigation plan was documented by URE. URE had a defense-in-depth security strategy, which included firewalls with port restrictions and deny-by-default access rules and an intrusion detection system with alerting enabled. All URE CIP Cyber Assets are within a secured ESP with real-time alerting and monitoring.

SERC determined the duration of the violation to be approximately six days, from the day after the initial security patch mitigation plan expired without URE applying the security patch or approving an extension to the mitigation plan through when the extension to the mitigation plan completion date was approved by the CIP senior manager's delegate.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the applicable personnel approve an extension to the patch mitigation plan;
2. Set reminders for mitigation plan due dates;
3. Built a spreadsheet to track all patch mitigation plans;
4. Trained relevant staff on the patch mitigation plan controls; and
5. Made a notification to all relevant staff reminding staff responsible for CIP patching of how to manage their patching mitigation plans.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017813 CIP-007-3a R6; R6.1 - OVERVIEW

SERC determined that URE failed to log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, cybersecurity Incidents. This violation involved two PCAs.

The cause of the violation was URE's product vendor's lack of awareness of the capabilities of a specific type of PCA.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to log events on the two PCAs could have hindered or prevented discovery of cybersecurity Incidents, or caused delays in the investigations of identified cybersecurity Incidents. Nevertheless, the two PCAs involved do not have any direct impact on URE operations or the BPS. URE uses these two PCAs to scan the network within the ESP for any new Cyber Assets. URE also utilizes an intrusion detection system with real-time alerting for any anomalous network activity. URE secures all Cyber Assets, including these two PCAs, within a defined ESP. Finally, after discovery of this capability to retain logs, URE was able to go back and review all logs dating back six months. URE found nothing suspicious in the logs that it was able to review.

SERC determined the duration of the violation to be approximately nine months, from the date URE put the PCAs into production without monitoring system events related to cybersecurity through when URE began pulling and retaining logs from the two PCAs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed an extent-of-condition review;
2. Obtained and reviewed logs for a specific device
3. Began frequently pulling and reviewing logs
4. Updated the security event log review procedure; and
5. Had the relevant department complete a read-and-sign of the updated event log review procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016605 CIP-007-6 R4; R4.4 - OVERVIEW

SERC determined that URE failed to review a sample of logged events in its automated security information and event management (SIEM) enterprise tool every 15 days to identify undetected cybersecurity Incidents on High Impact BES Cyber Systems and their associated EACMS and PCAs.

The cause of the violation was a failure to follow URE's procedure and lack of procedural controls.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to review and assess sample logs every 15 days could allow new or previously unidentified cybersecurity Incidents to go unrecognized for an extended time, delaying action to address the risk posed by a cybersecurity Incident. Nevertheless, URE was four days late in reviewing the log samples and did not identify any undetected cybersecurity Incidents in that review. URE also uses the automated SIEM tool for alerting for possible cybersecurity Incidents.

SERC determined the duration of the violation to be approximately four days, from the date a day after when URE should have conducted the 15-day assessment of event logs through when URE conducted the review of event logs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed the log upon discovery of the issue;
2. Created an automated recurring incident ticket that is automatically generated on a weekly basis;
3. Updated its security event log review procedure; and
4. Completed training for staff responsible for performing the CIP weekly log review procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017854 CIP-007-3a R5; R5.2.1 - OVERVIEW

SERC determined that in two instances URE failed to change passwords on administrator, shared, and other generic accounts prior to putting them into service in two separate instances when it could not remove, disable, or rename such accounts.

The cause of the first instance of the violation was a URE decision not to change the password as required, due to what URE deemed to be an unacceptable risk of opening up remote access and a lack of awareness of alternative options. The cause of the second instance was a failure of URE staff to follow the internal procedures, which require URE to change default accounts prior to installation.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's decision not to change default account passwords on certain Cyber Assets and its failure to explore possible work-arounds could have allowed a malicious actor to use well-known and widely distributed passwords to gain access to Cyber Assets within the URE network and thereby negatively affect URE operations or BPS reliability. Nevertheless, in the first instance, URE sought to reduce risk to the BPS by preventing remote access to the affected Cyber Assets. The second instance involved only two Cyber Assets. URE also utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately two years, from the date URE began deploying the Cyber Assets with default passwords installed through when URE changed the last default passwords on the Cyber Assets.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. For each new asset reviewed in the asset review meeting, gather information to capture if the asset has any default accounts and/or passwords;
2. Retrain relevant staff on the requirements of the system access control process;
3. Complete its extent-of-condition review;
4. Request and receive a position solution from the vendor to allow the password on a device to be changed without enabling remote access to the device;
5. Create an automated incident to notify the team when the next password change for a specific device is due;
6. Complete all troubleshooting with the vendor and testing;
7. Change the default password to the device on all machines that are CIP devices and have the agent installed;
8. Change the default passwords for multiple appliances; and

9. Create an automated notification to notify the team when the next password changes for the devices are due.

Mitigation activities for this violation are still ongoing.

SERC2016016607 CIP-007-3a R5; R5.3.3 - OVERVIEW

SERC determined that URE in three instances failed to enforce password changes technically or procedurally or enforce an obligation to change the password at least once every 15 calendar months for High Impact BES Cyber Systems and their associated EACMS, PACS, and PCAs.

The cause of the violation was a combination of inadequate controls and failure to follow URE's process requiring the change of passwords every 15 months.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to change passwords on an annual basis pursuant to CIP-007-3a R5.3.3 and at least every 15 months pursuant to CIP-007-6 R5.6 could have allowed malicious actors more time to guess or otherwise discover passwords. URE's failure to maintain evidence regarding the last password change for the Cyber Assets in the second instance of noncompliance increased the risk of the violation because URE had no evidence that it had ever changed those passwords, potentially leaving them vulnerable to guessing attacks for an extended period. Nevertheless, URE attested that all passwords in service in the three instances of noncompliance were sufficiently complex and at least eight characters in length, increasing the difficulty of guessing the passwords. In the first and second instances of noncompliance, 17 URE employees knew or could access these passwords, while in the third instance of noncompliance, only eight system administrators knew and could access this password.

SERC determined the duration of the violation to be approximately two years, from when URE should have had evidence of its compliance with CIP-007-3a through when URE changed the last password at issue in this violation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Changed relevant passwords;
2. Set up an automated incident ticket for the applicable accounts;
3. Revised the system access control procedure document;
4. Notified the relevant departments of the revisions to the system access control procedures;

5. Approved the assets and applications system access control revisions to the procedure document; and
6. Trained the relevant department on changes to the system access control procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016608 CIP-007-6 R5; R5.5 - OVERVIEW

SERC determined that URE failed to enforce the required password complexity on a device capable of supporting a password of at least eight characters and instead only used a password that was seven characters in length. A URE staff member scheduled a two-hour system outage in order to change its database account passwords after an employee transfer. After generating a random password to meet complexity requirements, the URE staff member inadvertently copied and pasted only seven of the eight-character password into the configuration files. Since the system masks the password, the URE staff member could not tell the error occurred. As an internal control as well as a programmatic password control, the URE staff member was required to paste the password into a database where a running script validated password compliance for complexity and length. In this instance, the script identified the password was seven characters instead of eight.

Security event logging was non-functional during the outage. Therefore due to the risk of possible reliability impacts due to an unplanned extended outage affecting its functions, URE staff decided not to extend the outage to make the necessary updates and scheduled a second system outage 15 hours later to update the password to the appropriate length.

The cause of this violation was insufficient training resulting in human error of placing a noncompliant password into the configuration files.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to have a password that met the length requirements could make it easier for a malicious actor to determine the password. Nevertheless, the noncompliant password was only in service for approximately 15 hours, and URE knew of the issue and scheduled a second outage to update the password to the appropriate length for the next day. Only two URE employees knew that a deficient password was in service, and only seven additional URE employees had access to the location where the password was stored.

SERC determined the duration of the violation to be approximately 15 hours, from when URE started operating with a database account password that was noncompliant through when URE resumed operations with a database account password that met the password length requirements.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Changed the password for the relevant database;
2. Updated procedures to clarify the password composition requirements; and
3. Notified the relevant departments of the password and procedure changes.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016610 CIP-007-6 R5; R5.7 - OVERVIEW

SERC determined that URE: (1) failed to limit the number of unsuccessful authentication attempts or generate alerts after reaching a threshold of unsuccessful authentication attempts for ten Cyber Assets because doing so was not technically feasible; and (2) did not request a TFE for those Cyber Assets.

The cause of the violation was a lack of sufficient process for requesting a TFE when limiting the number of unsuccessful authentication attempts or generating alerts after reaching a threshold of unsuccessful authentication attempts was not technically feasible.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to request a TFE when limiting the number of unsuccessful authentication attempts or generating alerts after reaching a threshold of unsuccessful authentication attempts was not technically feasible could have resulted in URE not implementing compensating measures to prevent a malicious actor from gaining unauthorized access through a password guessing attack or attempting to lock out an account through repeated authentication attempts. Nevertheless, although URE did not request a TFE as of the date of mandatory compliance, URE provided two attestations confirming that all compensating measures in the TFE that URE submitted to mitigate this violation had been in place since the time the Cyber Assets were placed into production. In addition, this violation only affected ten URE Cyber Assets that were protected within an ESP and PSP.

SERC determined the duration of the violation to be approximately five months, from the date the standard became mandatory and enforceable through when URE added the Cyber Assets to an existing CIP-007-6 R5.7 TFE.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Submitted a TFE for the devices which could not meet CIP-007-6 R5.7;
2. Approved a CIP asset classifications procedure;
3. Had relevant staff complete training on the CIP asset classification procedure;
4. Published its TFE procedure; and
5. Had relevant staff complete training on the TFE procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012682 CIP-009-3 R1 - OVERVIEW

SERC determined that URE failed to document recovery procedures adequately for all CCAs. The URE recovery plans only included discussion of common assets, workstations, consoles, and services but did not address other deployed CCAs within the ESP and did not provide sufficient detail on how to recover all classes of CCAs.

The cause of the violation was insufficient process and documentation. URE did not create recovery plans for CCAs that: (1) provided adequate information on how to recover all CCAs, (2) specified the required actions in response to conditions of varying duration and severity that would activate the recovery plan, or (3) defined the roles and responsibilities of responders.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to create adequate recovery plans for CCAs could delay the recovery of CCAs in the event that they became non-functional, thereby impairing URE's situational awareness of its portion of the BPS. Nevertheless, URE had high-level business continuity and restoration plans that could be used to assist in the recovery of CCAs. URE's subject matter experts likely had the technical expertise to recover CCAs in the event that they became non-functional, and URE had no need to recover CCAs during the period covered by the audit.

SERC determined the duration of the violation to be approximately five and-a-half years from the date the audit period began, through when URE implemented a revised BES Cyber Systems recovery plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented its BES Cyber Systems recovery plan pursuant to CIP-009-5 R1;

2. Held BES Cyber System recovery plan training for certain personnel;
3. Approved a new version of the BES Cyber System recovery plan; and
4. Conducted additional training on the BES Cyber System recovery plan.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2017017850 CIP-010-2 R1; R1.1 - OVERVIEW

SERC determined that URE failed to document all installed software on its baseline configurations in two instances.

The cause of the violation was a combination of insufficient training and insufficient internal controls to check and confirm baseline creation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to include custom software applications on the baseline for BES Cyber Assets and its omission of one BES Cyber Asset from a baseline entirely could have allowed undocumented changes to the baseline to go unnoticed and uninvestigated, potentially resulting in degradation of URE operations or the reliability of the BPS. Nevertheless, URE knew of custom-built software applications in the first instance and it required Active Directory access for logins, reducing the potential threat. URE was also able to provide evidence that it had tested the custom-built software when changes occurred, and that it periodically updated the software and tested it. One of the software applications was determined unneeded and unused since before the standard became mandatory and enforceable. For the second instance, URE omitted a single BES Cyber Asset from its baseline documentation for a period of approximately 10 months. URE also utilizes an intrusion detection system with real-time alerting for any anomalous network activity. URE secures all Cyber Assets within a defined ESP.

SERC determined the duration of the violation to be approximately ten months, from when the Standard became mandatory and enforceable through when URE completed documenting the last software application on its baseline documentation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Train relevant staff on the review process for checking and resolving issues with assets;
2. Complete training on baselining custom software applications for relevant staff;

3. Complete an extent-of-condition review;
4. Uninstall the software application that was not in use from the servers on which it was installed;
5. Update the baseline to capture the remaining software applications;
6. Reconfigure the automatic baseline collector for the missing Cyber Asset and collect the baseline configuration; and
7. Implement controls that include checking and resolving issues with assets.

Mitigation activities for this violation are still ongoing.

SERC2016016612 CIP-010-2 R1; R1.3 - OVERVIEW

SERC determined that URE failed to update the baseline configuration as necessary within 30 calendar days of completing the change for High Impact BES Cyber Systems and their associated PACs that deviated from the existing baseline configuration.

The cause of the violation was insufficient procedures and training resulting in the human performance failure of not following the document processes for updating baseline configurations within 30 days of the change.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to update its baseline configuration for High Impact BES Cyber Systems and associated PCAs within 30 days could have permitted stale documentation around configurations and versions of software to influence decisions that URE would make, potentially affecting URE's operations and security posture. The risk was elevated because the URE baseline owner responsible for baseline updates pursuant to CIP-010-2 R2.1 was not monitoring the automated tool that identifies changes to baseline configurations (see NERC Violation ID SERC2016016613). Nevertheless, this violation only affected approximately 1% of the total Cyber Assets. All changes at issue went through the appropriate change management process and were tested and approved. The Cyber Assets involved in this violation are mostly purpose-built with infrequent changes necessary. The Cyber Assets involved in this violation resided within secured PSPs and ESPs, both with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately five months, from the date 31 days after a change that deviated from the existing baseline configuration without URE updating the baseline configuration through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reconciled all outstanding changes to their respective baselines and promoted as appropriate for the device;
2. Implemented baseline exception reporting and escalation with asset exceptions report;
3. Revised the baseline configuration management process; and
4. Conducted training on the revised process for baseline owners.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017852 CIP-010-2 R1; R1.5 - OVERVIEW

SERC determined that URE, in three instances, failed to document test results and did not test all changes to High Impact BES Cyber Systems in a test environment or a production environment in such a way to minimize adverse effects prior to implementing a change in the production environment.

The cause of this violation was a lack of training on the change management procedures in instances one and three, and a failure by URE to understand and properly investigate the potential consequences of a change in instance two.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct testing prior to implementing a change in the production environment and its failure to retain test results of changes could result in operational impacts and make assessment of negative impacts difficult. Nevertheless, URE had internal controls in place that identified these failures within approximately a month at the longest, allowing URE to address any identified problems in a timely manner. URE utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP. URE did not experience any adverse effects or find any adverse impacts to its CIP-005 and CIP-007 cybersecurity controls as a result of the violation.

SERC determined the duration of the violation to be approximately four months, from when URE patched assets without retaining documentation of testing in the first instance through when URE discovered the third instance in which it did not document specific testing and save the results.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Complete its extent-of-condition review;
2. Make process and documentation updates to the baseline configuration change management procedure/process;
3. Train all relevant staff on the updated procedure and process;
4. Implement the change ticket review for CIP assets procedure; and
5. Complete training for relevant staff on the change ticket review for CIP assets procedure.

Mitigation activities for this violation are still ongoing.

SERC2016016613 CIP-010-2 R2; R2.1 - OVERVIEW

SERC determined that URE failed to monitor, at least once every 35 calendar days, for changes to the baseline configuration on High Impact BES Cyber Systems and their associated EACMS and PCAs. This violation involved the same Cyber Assets at issue in a CIP-010-2 R1.3 violation (NERC ID SERC2016016612). URE learned that the automated tool it used to conduct the automated comparison was identifying the change between the configuration running in the production environment and the documented configuration in the baseline, but the URE baseline owner responsible for baseline updates was not monitoring the application reporting tool dashboard for exceptions.

The cause of the violation was a combination of insufficient controls and human performance failure. URE did not have adequate controls in place to identify assets as the monitoring window was closing and did not notify and escalate to the appropriate staff for resolution. URE staff did not follow the established process and conduct the manual review of the dashboard showing changes to the baseline configurations.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor for changes to the baseline configuration running in production when compared to the documented baseline could have resulted in URE not noticing or resolving changes that had been made, either appropriate or malicious, possibly leading to operational impacts. Nevertheless, this violation only affected approximately 5% of the total Cyber Assets. All changes at issue went through the appropriate change management process and were tested and approved. The Cyber Assets involved in this violation are mostly purpose-built with infrequent changes necessary. The Cyber Assets involved in this violation resided within secured PSPs and ESPs, both with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately seven months, from the date 36 days after a change that deviated from the existing baseline configuration without URE investigating the change through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reconciled outstanding changes to their respective baselines, promoted, and where applicable, manually monitored;
2. Implemented CIP baseline exceptions and CIP baseline manual asset monitoring reports;
3. Revised the baseline configuration management process; and
4. Conducted training on the revised process for baseline owners.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

Operations and Planning Violations

URE's violations of the Operations and Planning Reliability Standards posed minimal risk to the reliability of the BPS. URE had protections in place that prevented elevated risk to the BPS, and no harm is known to have occurred from any of these violations. Specifically, URE would have responded to frequency deviations with a larger change in generation than it was required to provide. The larger contribution would tend to reduce the excursion, reduce the burden on neighboring registered entities, and assist in recovery of frequency. In addition, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. URE performed the required voltage analyses and found no conditions that required URE to establish different operating rules based on voltage. Finally, while URE's planning did not fully address performance requirements in the near-term and long-term planning horizons, URE addressed near-term and operational needs through other studies.

SERC2016015460 BAL-002-1 R4 - OVERVIEW

SERC determined that in two instances URE failed to recover its Area Control Error (ACE) within 15 minutes of the start of a Disturbance Control Standard (DCS) event.

The cause of the violation was an insufficient contingency reserve operating procedure and software system deficiencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to restore ACE to the required value within 15 minutes following two separate DCS events could result in prolonged operation at reduced frequency and reliance on neighboring registered entities to provide generation to balance the load. Nevertheless, URE restored ACE within five minutes of the required recovery period for each instance. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two minutes and five minutes, from 15 minutes after the start of the Reportable Disturbance through when URE returned its ACE to zero.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Ensured it carried additional contingency reserves for three months, as required by the BAL-002 Standard for failure to meet the Disturbance Control Standard (DCS) criteria 100% of the time;
2. Installed two patches to applicable software systems to (a) correct system user interface issues; and (b) correct an operational issue;
3. Revised its contingency reserve operating procedure to reflect changes necessary to prevent a recurrence of delayed response to a DCS event; and
4. Completed training on the contingency reserve operating procedure.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016016157 BAL-003-1.1 R2 - OVERVIEW

SERC determined that URE failed to implement a revised Frequency Bias Setting (FBS) according to the assigned schedule. URE stated that it was aware of the impending implementation and its staff awaited the ERO posting notification. URE also stated that it did not receive notification of the posting or the FBS by the required implementation date.

The cause of the violation was human performance and lack of awareness. URE did not update its FBS in accordance with the implementation plan because it was not aware of the location of the revised FBS settings.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to implement correct FBS may result in an inaccurate calculation of ACE and related Control Performance Standards (CPS). In the short term, it could result in a reduced response from URE during a frequency excursion. In the long term, it could result in URE failing meet its

interchange responsibilities. Nevertheless, URE would have responded to frequency deviations with a larger change in generation than it was required to provide. The larger contribution would tend to reduce the excursion, reduce the burden on adjacent entities, and assist in recovery of frequency. URE addressed any Inadvertent Exchange resulting from the incorrect Frequency Bias on an hourly basis throughout the period. The calculation of CPS is a monthly requirement. While the Frequency Bias error existed for more than one month, CPS is calculated on a monthly basis and URE took slightly longer than a month to implement the revised FBS, so its effect on the calculation of CPS was minimal. No frequency excursions during the period are attributable to the incorrect Frequency Bias. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately one month, from the day after URE was required to implement the revised FBS through when URE implemented the revised FBS.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Immediately adjusted the Frequency Bias Setting in the URE ACE calculation, after confirming the validation of the new Bias settings with the ERO;
2. Approved revisions to the operations process document to reflect changes in the BAL-003 Standard relating to the changing of the FBS;
3. Had all staff in the relevant department complete a read-and-sign of the updated version of URE's Frequency Bias Adjustment Procedure; and
4. Employed multiple calendar reminders leading up to and shortly after the annual requirement dates for updating the Frequency Bias to remind multiple URE staff of the need to change the setting in a timely fashion.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015526 FAC-014-2 R3 - OVERVIEW

SERC determined that URE failed to produce evidence that it performed voltage stability analyses when establishing SOLs as required by its SOL methodology.

The cause of this violation was URE's lack of a documented process and schedule, and insufficient training and internal controls to ensure that personnel performed and retained evidence of the voltage stability analyses required by URE's SOL methodology.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its SOL methodology to establish SOLs for at least three-and-a-half years could result in URE entering unsafe operational configurations that could damage equipment or cause system instability. Additional facts helped mitigate the risk of the violation. Although URE had not established SOLs based on voltage stability analyses, it performed contingency analyses that included voltage considerations. As a result, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. After discovering the violation, URE performed the required voltage analyses and found no conditions that required URE to establish SOLs based on voltage. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately three-and-a-half years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the TPL-001-4 study to identify any potential voltage issues starting in the summer of the following year and found none;
2. Approved its TPL-001-4 steady state procedure, which documents the steps necessary to analyze the non-converged contingencies that may identify potential voltage issues;
3. Developed its FAC-014-2 process document to assist staff in compiling the list of established SOLs/Interconnection Reliability Operating Limits (IROLs). Specifically, outlined the review process for non-converged contingencies identified in the TPL-001-4 Planning Assessment and the inclusion of the identified facilities in the SOL/IROL list;
4. Developed detailed project schedules documenting future requirements and due dates. Specifically, created tasks in project schedules to incorporate non-converged contingency analysis, compliance checkpoints, and the posting of SOL/IROLs;
5. Provided updated schedules and documentation to the appropriate subject matter experts for review and acknowledgement;
6. Provided training on solutions for non-converged contingencies to the appropriate subject matter experts;
7. Developed a TPL-001-4 stability process document covering any additional SOLs that resulted from the stability study; and
8. Provided updated TPL-001-4 stability process document for subject matter expert review and acknowledgement.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015527 FAC-014-2 R4 - OVERVIEW

SERC determined that URE failed to produce evidence that it performed voltage stability analyses when establishing SOLs as required by the Planning Authority's SOL Methodology.

The cause of this violation was URE's lack of a documented process and schedule and insufficient training and internal controls to ensure that personnel performed and retained evidence of the voltage stability analyses required by the Planning Authority's SOL methodology.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its Planning Authority's SOL methodology to establish SOLs for at least three-and-a-half years could result in URE entering unsafe operational configurations that could damage equipment or cause system instability. Additional facts helped mitigate the risk of the violation. Although URE had not established SOLs based on voltage instability, it performed contingency analyses that included voltage considerations. As a result, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. After discovering the violation, URE performed the required voltage analyses and found no conditions that required URE to establish SOLs based on voltage. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately three-and-a-half years from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the TPL-001-4 study to identify any potential voltage issues starting in the summer of the following year and found none;
2. Approved its TPL-001-4 steady state procedure, which documents the steps necessary to analyze the non-converged contingencies that may identify potential voltage issues;
3. Developed its FAC-014-2 process document to assist staff in compiling the list of established SOLs/ IROLs. Specifically, outlined the review process for non-converged contingencies identified in the TPL-001-4 Planning Assessment and the inclusion of the identified facilities in the SOL/IROL list;

4. Developed detailed project schedules documenting future requirements and due dates. Specifically, created tasks in project schedules to incorporate non-converged contingency analysis, compliance checkpoints, and the posting of SOL/IROLs;
5. Provided updated schedules and documentation to the appropriate subject matter experts for review and acknowledgement;
6. Provided training on solutions for non-converged contingencies to the appropriate subject matter experts;
7. Developed a TPL-001-4 stability process document covering any additional SOLs that resulted from the stability study; and
8. Provided updated TPL-001-4 stability process document for subject matter expert review and acknowledgement.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2017016808 PRC-002-2 R5; R5.3 - OVERVIEW

SERC determined that URE failed to notify one Transmission Owner, within 90 calendar days of completion of Part 5.1, that certain BES Elements required dynamic Disturbance recording (DDR) data.

The cause of this violation was insufficient procedures and training resulting in the human error in communicating incorrect information.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to notify a Transmission Owner that certain of its BES Elements required DDR data could result in insufficient data to analyze a disturbance on the BPS. Nevertheless, DDRs are used for forensic analyses following a disturbance and do not affect real-time operation or long-term or short-term planning of the BPS. While URE notified the Transmission Owner that certain of its BES Elements required DDR data approximately 40 days late, Transmission Owners have four years to reach 50% compliance and six years to reach full compliance with the installation requirements. This violation did not cause or prevent a disturbance, and the Transmission Owner did not receive a request for the DDR data to analyze a disturbance during this violation. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately 40 days, from the day after URE should have notified the Transmission Owner that DDR data was required through when URE notified the Transmission Owner that DDR data was required.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Notified the Transmission Owner in question that DDRs are necessary;
2. Updated its PRC-002-2 procedure to include an additional verification of the list of affected Transmission Owners;
3. Added tasks to the PRC-002-2 annual project plan to address this new step; and
4. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and procedure.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015697 PRC-023-3 R6 - OVERVIEW

SERC determined that URE failed to apply criterion B4 in Attachment B to the assessment it conducted in a single year. SERC later determined that URE also did not conduct an assessment within the prior calendar year, and thus did not apply any of the criteria in Attachment B in that calendar year. URE was not aware of the requirement to perform an assessment at least once each calendar year, but did perform its next assessment within 15 months of the prior assessment.

The cause of this violation was an inadequate process and deficient procedures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to identify low voltage transmission lines that may need to operate under temporary overload during contingencies may exacerbate those events. In this case, URE had performed the other required assessments in the second year and had informed the affected Transmission Owners of transmission lines requiring set point reviews. When URE completed the criterion B4 analyses, it determined that approximately 6% of the lines no longer met the criteria and 0.6% of the additional lines met the criteria requiring reviews. URE provided the revised list of circuits to all relevant parties within 30 days. The newly added transmission lines only met the B4 criterion under certain multiple contingency conditions. Since circuits identified through the criterion B4 analyses were related to the one-to-five year planning horizon, the delayed assessment did not result in an imminent risk to the BPS. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately five months from the date after the last date URE should have performed the assessment within the calendar year, through when URE completed the assessment that included the required criterion B4 analyses.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed its annual assessment including the B4 assessment, which is within the required calendar year, not to exceed a 15-month timeframe;
2. Added compliance checkpoints into the resource project schedules;
3. Updated the annual schedule with a log to capture milestone completion dates;
4. Created detailed annual and monthly checklists, including appropriate annual and monthly checkpoints according to PRC-023-3 R6;
5. Updated its PRC-023 process document, which includes references to the annual and monthly checklist; and
6. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and process documentation.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015532 TPL-002-0b R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not demonstrate that system performance met all Category B contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category B contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not demonstrate that system performance met all Category B contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE analyzed system

configurations similar to these Category B contingencies during contingency analyses, and would have identified problems in the short-term planning and operating horizon. URE's assessments did not demonstrate that system performance met Category B contingencies for a small number of Category B contingencies that typically do not present a large risk to the BPS. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;
5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015533 TPL-003-0b R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not demonstrate that system performance met all Category C contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category C contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not demonstrate that system performance met all Category C contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE addressed near-term and operational needs through other studies. URE assessments did not demonstrate that system performance met Category C contingencies for a relatively small number of Category C contingencies, which have a low probability of occurring. Consideration of system response to Category C contingencies is only part of the assessment process. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;

5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015534 TPL-004-0a R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not show system performance following all Category D contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category D contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not show system performance following all Category D contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE addressed near-term and operational needs through other studies. URE assessments did not show system performance following the relatively small number of Category D contingencies, which have a low probability of occurring. Consideration of system response to Category D contingencies is only part of the assessment process. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;
5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of five hundred thousand dollars ($500,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. The instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE admitted to the violations and accepted responsibility for them;
3. URE agreed to the following changes to its organizational matrix and compliance culture:
    a. Reassigning the role of the CIP senior manager.
    b. Formation of a new group whose sole responsibility is the security of URE's Cyber Assets. This team performs URE's active CVA yearly.

c. Formation of a certain group whose responsibility is to oversee the quality of the work conducted by IT.

d. Reorganization of a relevant department such that it is no longer responsible for the security of URE's assets. It now concentrates its efforts on compliance matters and advising IT. The relevant department hired a new manager; this allowed the upper management of the department to focus on strategic matters rather than day-to-day operations.

e. Hired a CIP compliance subject matter expert with years of experience. This individual brought a different perspective to URE that has allowed it to enhance its compliance culture.

f. Shifted ownership of compliance responsibility from the compliance group to IT subject matter experts—removing the past practices of the compliance group being a buffer between subject matter experts and auditors.

g. Developed a program to encourage its employees to proactively identify and report potential violations of NERC Reliability Standards.

4. URE had an internal compliance program at the time of the violations, but SERC determined that, given the difficulties described above, the quality of URE's compliance program was deficient in demonstrating URE's compliance with the CIP standards and requirements. Therefore, SERC considered it to be a neutral factor;

5. URE's lack of cooperation and failure to timely submit its Mitigation Plans, failure to timely complete its Mitigation Plans, and failure to provide adequate evidence of completion of Mitigation Plans;

6. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. Although the risk posed to the BPS by the individual violations ranged from minimal to serious (26 minimal, 28 moderate, and 5 serious), the collective risk of the 59 violations posed a serious risk to the reliability of the BPS; and

8. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of five hundred thousand dollars ($500,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 8, 2017 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of five hundred thousand dollars ($500,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

[4] *See* 18 C.F.R. § 39.7(d)(4).

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

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

James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Holly A. Hawkins* General Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 357-7914 – facsimile hhawkins@serc1.org Gary J. Taylor* President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8205 (704) 357-7914 – facsimile gtaylor@serc1.org	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Anne Faugust* Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Timothy E. Ponseti* Vice President, Operations SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8202 (704) 357-7914 – facsimile teponseti@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Leigh Anne Faugust
Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation