

**COMMONWEALTH OF KENTUCKY**  
**BEFORE THE PUBLIC SERVICE COMMISSION**

In the Matter of:

The Application of Kentucky Power Company for: )  
(1) A General Adjustment of Its Rates for Electric )  
Service; (2) An Order Approving Its 2014 ) Case No. 2014-00396  
Environmental Compliance Plan; (3) An Order )  
Approving Its Tariffs and Riders; and (4) An Order )  
Granting All Other Required Approvals and Relief )

**NERC COMPLIANCE AND CYBERSECURITY DEFERRAL REPORT**

Kentucky Power submits the following annual report pursuant to the Commission's June 22, 2015 Order in Case No. 2014-00396:

Paragraph 14(c) of the Settlement Agreement in Case No. 2014-00396, as approved by the Commission, provides:

Kentucky Power agrees beginning on or before March 31, 2016, and each March 31<sup>st</sup> thereafter, it shall make an informational filing with the Commission quantifying and describing the amounts deferred in accordance with this paragraph 14. A copy of this annual informational filing shall be served by Kentucky Power upon counsel for all parties to this proceeding.

During calendar year 2020, the Company continued to incur incremental costs for work orders (projects) to comply with NERC compliance or cybersecurity requirements established subsequent to the Commission's Order in Case No. 2014-00396. These projects are:

- W/O SITC056001 - NERC-CIP v5 Upgrade - Program Management team costs for upgrades to systems and processes to enable readiness for the new v5 NERC CIP standards. (Closed 2017)
- W/O SITC151801- ECMP Agile Team - ECMP (End Point Configuration Management) costs needed to support NERC CIP v5 Upgrade Program. (Closed 2017)
- W/O SITC152301 – Security Configuration Agile Team - Implementation of new

tool “iDefender” to enable compliance with new NERC CIP v5 Configuration Management requirements. (Closed 2017)

- W/O SITC151901 – Firewall Management Tool Team - Implementation of new tool “Tufin” to enable compliance with new NERC CIP v5 Firewall Management requirements. (Closed 2017)
- W/O SITC151701 – ARCS Agile Team – ARCS (AEP’s Risk & Compliance Solution) updates needed to support new NERC CIP v5 requirements. (Closed 2017)
- W/O SITC152401 – ServiceNow Agile Team – ServiceNow updates needed to support new NERC CIP v5 requirements. (Closed 2017)
- W/O SITC152101 – IAM Agile Team – IAM (Identity & Access Management) updates needed to support new NERC CIP v5 requirements. (Closed 2017)
- W/O SITC156201 – IT Active Directory – Implementation of a new active directory domain to support new NERC CIP v5 requirements. (Closed 2017)
- W/O SITCB44601 – Physical Access Control – Implementation of new Physical Access Control System for NERC CIP v5 requirements. (Closed 2018)
- W/O SITCA40401 – Physical Access Management – Implementation of a new system for physical access management for NERC CIP v5 requirements. (Closed 2017)
- W/O SITCA55601 – PAM Cost for EACMS – Additional costs needed for implementation of a new system for physical access management (PAM) for NERC CIP v5 requirements surrounding EACMS (Electronic Access Control and Monitoring Systems). (Closed 2017)
- W/O SITCB45901 – Lenel OnGuard Upgrade – Implementation of new Physical Access Control System (Lenel OnGuard) for NERC CIP v5 requirements. (Closed 2017)
- W/O SITCQ16201 – Cyber – Intrusion Detection (Cisco Enhancements) - This initiative will increase the capabilities of Cisco tools for cyber security and resolve issues with proxies which is how users route to the Internet. (Closed 2018)
- W/O SITCQ26001 – Cyber – Cisco Security Enterprise License Agreement – Upgrade the existing 5-year Enterprise License Agreement (ELA) from version 4 to version 5. (Open)
- W/O SITCQ04501 – Cyber – Access Control Enhancements - This project is part of the 2017 Cyber Security Investment to enhance existing enterprise cyber security

capabilities and implement security tools to meet emerging needs. This initiative will remediate audit findings and address access management system pain points identified during in-flight projects. (Closed 2019)

- W/O SITCQ16001 – Cyber – McAfee Health and Expansion - This initiative will upgrade all current existing products in the CORP ePO, McAfee ePolicy Orchestrator, infrastructure to expand capabilities; upgrade the Supervisory Control and Data Acquisition, SCADA, ePO infrastructure; and separate SCADA, Commercial Operations, and NERC-CIP, North American Electric Reliability Corporation Critical Infrastructure Protection assets into the SCADA ePO infrastructure, and all other assets into the CORP infrastructure. This project will also remediate any security gaps identified in endpoint configurations. (Open)
- W/O SITCQ05301 – Cyber – Vulnerability Management Tools - This project is part of the 2017 Cyber Security Investment to enhance existing enterprise cyber security capabilities and implement security tools to meet emerging needs. This initiative will deploy new software and scanners to increase the capabilities of the vulnerability management program. (Closed 2018)
- W/O SITCQ05001 – Cyber – Security Tools for Testing and Assessment – This project is part of the 2017 Cyber Security Investment to enhance existing enterprise cyber security capabilities and implement security tools to meet emerging needs. This initiative will provide new security tools for testing and assessments; augment hardware testing capabilities; and equip the cyber team with tools to conduct effective penetration testing for new software/hardware. (Closed 2018)
- W/O SITCR11401 – Cyber – Access Reconciliation Setup - Each Business Unit will be responsible for the daily access reconciliation of their applications, implementing this project will assist them with the required tools to help meet this new cyber security standard. Several vendors will provide professional services to assist AEP in obtaining the required data, and assist in the reconciliation setup of their externally hosted application. (Open)
- W/O SITCQ16701 – Cyber – Enterprise Password Authentication Program – Phase 2 - This initiative will address high-priority enhancements to AEP identity and access control applications. (Closed 2020)
- W/O SITCR23901 – Cyber BUO – Cybersecurity Tools and Software - This project will fund the capital purchase of Cybersecurity testing tools and additional software needed that will help AEP stay ahead of malicious attacks and enable the ability to neutralize any threats in a more prompt and efficient manner. (Open)
- W/O SITCR25501 – Cyber – 2018 Phishing Training and Awareness - This effort will put in place education-based policies, procedures and awareness measures to ensure staff have a common understanding of what Cyber phishing attacks are, how

to recognize them, and what to do in the event they receive one. (Open)

- W/O SITCR33901 – Cyber – CyberArk – AIM (Application Identity Manager) - This project is to purchase and implement CyberArk Application Identity Manager, AIM, module for 300 application servers as well to purchase and implement a test environment for CyberArk Vault. (Open)
- W/O SITCS22201 – Cyber – DPPG Data Governance and Compliance Program - Implementation of a data governance toolkit that will help AEP Business Units analyze their data assets for quality relationships and then leverage that data for greater business benefit. (Open)
- W/O SITCS23001 – Cyber – SOAR Phase 2 - Build additional automation functionality in the Security Orchestration, Automation and Response, SOAR, platform to address cyber incident response tasks. (Closed 2021)
- W/O SITCS34201 – Cyber – Fidelis Upgrade - Purchase and deploy Fidelis appliances and licensing at NADC and Tulsa. Key project tasks include: 1. Replace all Fidelis equipment: includes sensors, collectors and controllers 2. Develop granular alerting of security events on network traffic flows 3. (Open)
- W/O SITCS32901 – Cyber – Contrast Application Security - We will purchase and deploy Contrast Security Assess agents for up to 61 application Dev Test QA environments. These agents will allow us to integrate security testing into the functional testing pipeline. (Open)
- W/O SITCS37701 – Cyber – DPPG Data Governance and Compliance Program - This project will purchase and deploy new application modules for ARCs, Guardium, IBM StoredIQ, and McAfee DLP Discovery and purchase additional licenses and additional appliances for IBM's Guardium tool. AEP teams will contract with several vendors for these different applications to assist with configuration, implementation and deployment. (Open)
- W/O SITCS38701 – Cyber – Outbound Decryption - This project is to purchase and implement an F5 Orchestrator and other F5 equipment such as Transceivers at AEPs New Albany Data Center and at the Tulsa Data Center. (Open)
- W/O SITCS44101 – Cyber – Network Defense Upgrades 2019 - This project will replace obsolete Cisco network sensors across the enterprise as well as network bypasses and replace and upgrade AEPs network aggregators at the New Albany Data Center. (Open)
- W/O SITCS49801 – Cyber – McAfee SLA - This project will update and implement all of the tools identified in the McAfee Strategic License Agreement which includes a suite of endpoint security products, cloud security tools, data



discovery tools, advanced threat detection, mobile protection and web gateway products. (Open)

- W/O SITCS54901 – Cyber – Security Analytics - This project will install the hardware and software needed and define the process/procedures to provide predictive analytics, assisting AEP in identifying and mitigating threats. (Open)
- W/O SITCS55001 – Cyber – Audit Remediation - This project will develop and deploy new functionalities in ServiceNow, and enhance existing functionalities within applications/tools such Archer, aka ARCs, MyAccess, Boldon James Classifier and IBM Guardium. AEP teams will contract with several vendors for these different applications to assist with configuration, implementation and deployment. (Open)
- W/O SITCS61001 – Cyber – CyberArk PW Vault - The IT Risk Management team has identified an opportunity to remediate an audit finding by deploying an enterprise password vault solution for NERC CIP and SOX governed applications. CyberArk Enterprise Password Vault (EPV) is a suite of applications that securely manage passwords and other related sensitive objects. While it is typically used to store and manage privileged account passwords, it has the capability to verify and auto rotate passwords. This solution has been successfully set up for corporate use. This project will replicate the system to provide the same level of security for NERC CIP systems that run in areas logically cordoned off from AEP's production environment. As part of this project we will onboard all SOX and NERC CIP passwords into the vaults and determine a way to change these passwords. (Open)
- W/O SITCS62101 – Cyber – Access Control Investment 2020 - The scope is to build Internet of Things networks, enhance mobile device management integration for wireless devices, implement Public Key Infrastructure and authentication. (Open)
- W/O SITCT33101 – Cyber – VulnextPh2ConfigMgt – This project will enhance the VulNEXT program with new configurations and purchases for additional tenable licenses, new modules for identifying security vulnerabilities and automating manual tracking processes. (Open)
- W/O SITCS49401 – Cyber – MDR (Monitoring, Detecting and Responding) - AEP is purchasing multiple applications for the Cybersecurity Incident Response Center, aka CIRC, to replace the loss of incident response, alert management, threat hunting, threat intelligence, quick indicator triage for historical activity, advanced file analysis and advanced mail triaging capabilities that are end of life and no longer going to be supported to continue monitoring, detecting and responding, aka MDR, to threats. (Open)

The Company completed work and closed out eighteen of the 37 projects listed above over

the course of 2017, 2018, 2019 and 2020. Nineteen projects remain open.

In Case No. 2017-00179, Kentucky Power sought and received Commission approval to amortize and recover over five years the deferred costs related to the NERC Compliance and Cybersecurity projects booked between the Commission's June 22, 2015 Order in Case No. 2014-00396 and February 28, 2017, the end of the test year in Case No. 2017-00179.

The total deferred depreciation expense (\$496,445)<sup>1</sup> and carrying charge (\$202,064)<sup>2</sup> amounts incurred between the end of the test year in Case No. 2017-00179 (February 28, 2017) and the end of calendar year 2020 is \$698,509. The support for the deferred depreciation expense calculation is shown on **EXHIBIT NERC-1** attached to this report. The support for the calculation of the deferred carrying charge is show on **EXHIBIT NERC-2**. No operation and maintenance expense was incurred related to these projects.

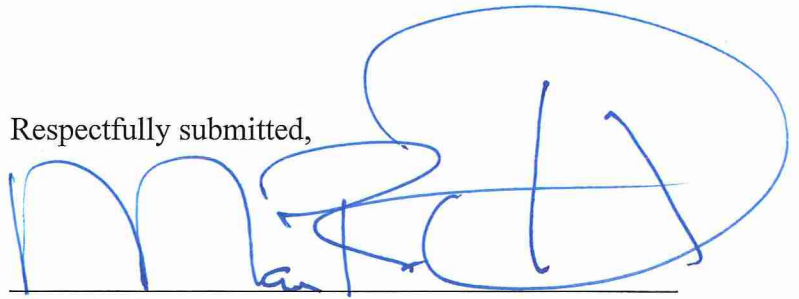
Kentucky Power proposes beginning with it calendar year 2021 report (to be filed in 2022) to delete from the report those projects that were previously reported as closed in a calendar year prior to the calendar year of the report.

---

<sup>1</sup> See "Total" line of column (V) ("Previous Months Retail Share of Accumulated Depreciation") of **EXHIBIT NERC 1**.

<sup>2</sup> See "Total CC" column of **EXHIBIT NERC 2**.

Respectfully submitted,



Mark R. Overstreet

Katie M. Glass

STITES & HARBISON PLLC

421 West Main Street

P.O. Box 634

Frankfort, Kentucky 40602-0634

Telephone: (502) 223-3477

Facsimile: (502) 779-8349

[moverstreet@stites.com](mailto:moverstreet@stites.com)

[kglass@stites.com](mailto:kglass@stites.com)

Counsel For Kentucky Power Company