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 Environmental Compliance Plan; (3) An Order Approving Its Tariffs and Riders; and (4) An Order Granting All Other Required Approvals and Relief	))))))	Case No. 2014-00396

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 31st 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 2021, 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 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 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 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. (Closed 2021)

- 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. (Closed 2021)

- 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 IBMs 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. (Closed 2021)

- 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. (Closed 2021)

- 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. (Closed 2021)

- 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)

- W/O SITCU31901 – Cyber – ICS OT Network Sensor - AEP Cybersecurity has been developing requirements and researching Industrial Control Systems (ICS)/ Operational Technology (OT) network sensor vendors for the past two years. This project will purchase and deploy network sensors to critical AEP facilities/locations as well as a data diode appliance as a compensating control for NERC CIP. (Open)

- W/O SITCU36101 – Cyber – Central Repository - Extends File Integrity Assurance and central repository for software, firmware and patches beyond the NERC CIP area to include verification of source and integrity of files retrieved from outside AEPs network. (Open)

- W/O SITCV16801 – Cyber – HVA Phase 2 - This capital work will expand AEP High Value Asset (HVA) inventory through the ServiceNow platform by identifying, inventorying, and providing a systematic accountability through certification for two additional data types (Regulatory and Legal). It will include building out the necessary attributes about the HVA data in areas around protection controls, storage, configuration item connections and external data sharing. It will also expand the capabilities of ServiceNow to allow data custodians and data owners to electronically validate and certify their HVA data sets through the ServiceNow HVA Portal. (Open)

- W/O SITCU06201 – Cyber – IAM Access Enhancements- This project is to enhance the essential Access Control and Enterprise Authentication Framework tools (EAF) (MyAccess, IDVerify, iForgot, Adaptive Authentication and IAR (Infrastructure Access Repository) - aka: ECMP replacement) as well as supporting policies/processes and Organizational Change Management (OCM) needed to meet emerging business and compliance needs in the IAM space. It will also engage some professional services as well as purchase RSA soft and/or hard tokens to ensure external access can be securely and properly obtained. (Open)

- W/O SITCU15801 – Cyber – IAM EAF - This work order is specifically for the EAF Agile team for capital work on the tools (IDVerify, iForgot and Adaptive Authentication) their line is responsible for. The project as a whole is to enhance the essential Access Control and EAF tools as well as supporting policies/processes and OCM that is needed to meet emerging business and compliance needs in the IAM space. It will also engage some professional services as well as purchase RSA soft and/or hard tokens to ensure external access can be securely and properly obtained. (Open)

- W/O SITCU15901 – Cyber – IAM Program - This work order is specifically for the program team for capital work on Identity Access Management (IAM). The project as a whole is to enhance the essential Access Control and EAF tools as well as project management specific policies/processes and OCM needed to meet emerging business and compliance needs in the IAM space. It will also engage some professional services as well as purchase RSA soft and/or hard tokens to ensure external access can be securely and properly obtained. (Open)

- W/O SITCU25901 – Cyber – VulNEXT DAVE Renewal - Cybersecurity will renew licenses of the Fortress Data Analytics Vulnerability Engine, DAVE, for two years to include installation, configuration, development and customization and support services for the DAVE Tool along with knowledge transfer and roll out of new features and functionalities. (Open)

- W/O SITCU52701 – Cyber – Splunk - This project will purchase enough licenses to allow AEP to use Splunk as its enterprise SIEM. Splunk will improve on the current SIEM by enabling faster searches for incident response and application health monitoring, allowing the creation of real time dashboards for application and cyberattack monitoring, improve cybersecurity automation and orchestration, and help AEP comply with regulations requiring log storage. (Open)

The Company completed work and closed out six of the projects listed above over the course of 2021. Twenty-two 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 ($1,107,161)[1] and carrying charge ($368,967)[2] amounts incurred between the end of the test year in Case No. 2017-00179 (February 28, 2017) and the end of calendar year 2021 is $1,476,128. 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.

Respectfully submitted,

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
kglass@stites.com

Counsel For Kentucky Power Company

[1] *See* "Total" line of column (W) ("Previous Months Retail Share of Accumulated Depreciation") of **EXHIBIT_NERC_1**.

[2] *See* "Total CC" column of **EXHIBIT_NERC_2**.