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

2023 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 2023, 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. (Closed)
- 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. (Closed)

- 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. (Closed)

- 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. (Closed)

- 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. (Closed)

- 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 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. (Closed)

- 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 SITCT49401 – 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. (Closed)

- 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. (Closed)

- 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. (Closed)

- 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. (Closed)

- 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)

- W/O SITCV11401 – Cyber-Network Defense 2022 - This capital effort is needed to enhance alerting and incident response, implement redundancy for critical applications and increase visibility into areas that we do not currently have it. It includes purchasing some new security tools (IXIA CloudLens, FireEye FX) (Closed)

- W/O SITCV17501 – CyberSCM-CIPSNOWAutomation - This project is to create forms and automate processes and workflows in ServiceNow to build (commission) and retire (decommission) the different types of NERC CIP devices supported by AEP Technology and Security organization (in order to comply with new NERC CIP standards.) (Closed)

- W/O SITCU51101 – Cyber-SCM-CognoseCIPRpting - Using COGNOS, integrations will be built from 20+ technology & security source systems to (1) create new controls to maintain AEP's compliance with NERC CIP standards, (2) demonstrate controls are operating effectively and (3) to automate the submission of evidence to NERC regional auditors where audits are conducting on an increasing frequency. (Open)

- W/O SITCV29301 – Cyber-DataProtectionPhase2 – Enhanced AEP Classifier tool to support Regulatory Compliance data types as well as MP-511. Enhanced McAfee Suite of products to support additional HVA data types through rules for discovery and scanning. DLP tools matrix for action (quarantine, block, monitor, etc.) will support new HVA data types for Regulatory Compliance. Applicable roles and entitlements will be identified and edited to support additional data types with appropriate review cadence, descriptions, provisioning, and compliance flags. Identification and implementation of native encryption, where available, for each new HVA data type as well as any in-motion encryption/protection controls for data transmission outside of AEP (SFTP, TLS, other). (Open)

- W/O SITCV34201 – PSEC-OnGuard Upgrade 2022 - OnGuard is an enterprise wide physical security application that is used to monitor and control card reader access to AEP's buildings and facilities (including NERC CIP locations-rooms). The current version (7.5) is currently out of support. This effort will upgrade to version 8.1 and include new features-functionality such as encryption. It will separate web clients for NERC CIP and non-NERC CIP. (Open)

- W/O SITCV37001 – Cyber -OT Forensics - This new solution within OT will allow for a more immediate response and reduce the need for emergency change requests during an incident, enhance collection reliability, prevent unnecessary firewall connections between corporate and OT in an incident or investigation, allow us to

perform analysis within the OT environment (without moving volumes of data into corporate analysis systems) which results in faster analysis and reduced processing time. The project will largely improve Cyber's capability to respond in an incident or investigation, supports business growth and improves operational efficiencies. (Closed)

- W/O SITCV38001 – Cyber-M365AlertingResponse - Enabled M365 logging and alerting integrated with the CIRC's SIEM, alert management solution and workflow processes. Discovery, validation, change recommendation of M365 DLP strategy.
    - M365 alerting requirements defined
    - High fidelity alerting created by integrating and combining data from M365 and multiple existing security technologies flowing to the CIRC's Case Management system
    - Develop, optimize and operationalize playbooks to address alerts using automation whenever possible
    - Security analysts are trained in m365 monitoring needs and maintenance of created alerting and automations
    - Review, document and make recommendations for DLP strategy in M365 prioritizing existing solution capabilities (Closed 2023)

- W/O SITCV23501 – Cyber-VulNEXT 2022 - Inventory will be collected, responsible parties will be identified for all critical applications in those areas, and full vulnerability monitoring, analysis, dispositioning, and tracking will be established. We will have secure configurations deployed for new builds on the technology stacks above and monitoring will commence to ensure that the configurations deviate from the approve standard. (Open)

- W/O SITCW22501 – Cyber-IAM Program Enhancements 2023 – Ongoing efforts to continuously improve the Identity and Access Management (IAM) program with a variety of enhancements that include: privileged access management in CyberArk, certification reviews and recon processes in MyAccess, forms and workflows in ServiceNow (UAUR – User Access User Requests), Robotic Automation (RPA for ITAMBOT) and any others that are necessary to remediate audit findings and mitigation plans for SOX and NERC/CIP. (Open)

- W/O SITCW31001 – Cyber – Fidelis Lifecycle Upgrades – Upgrades all current Fidelis network equipment to keep pace with bandwidth increases therefore ensuring the solutions continued ability to monitor and detect malicious activity. Also includes purchases and implementation of Sandbox Malware Automation Disposition and Triage for malware detection that runs a suspicious object in a virtual machine to detect malicious behavior. (Open)

- W/O SITCW31301 – Cyber VULNEXT Enhancement 2023 – This effort will maintain compliance with NERC CIP regulatory requirements by renewing our VulnDB contract-licenses for three years and implementing any new

features/functionality that are included as well as creating a new lower environment for tenable scanning environment. Additional enhancements will be completed to expand configuration management into our enterprise infrastructure (Oracle, SQL, DB2, Windows Server 2016, and Windows 2019). (Open)

- W/O SITCW34401 – Cyber HVA – Phase 3 – Continuation of the HVA (High Value Assets) journey to enhance ServiceNow to support two new data types (Cybersecurity Information and Customer Data), implement annual certification and modify workflows-integrations to ensure proper data protection controls are in place. (Open)

The Company completed work and closed out 14 of the projects listed above over the course of 2023. Fourteen projects remain open.

In Case No. 2020-00174, 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 January 18, 2018 Order in Case No. 2017-00179 and March 31, 2020, the end of the test year in Case No. 2020-00174. In Case No. 2023-00159, 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 January 13, 2021 Order in Case No. 2020-00174 and March 31, 2023, the end of the test year in Case No. 2023-00159.

The total deferred depreciation expense ($575,824)[1] and carrying charge ($165,674)[2] amounts incurred between the end of the test year in Case No. 2023-00159 (March 31, 2023) and the end of calendar year 2023 is $741,498. The support for the deferred depreciation expense calculation is shown on **EXHIBIT NERC-1** attached to this report. The support for the

[1] *See* "Depreciation Expense for period April 1, 2023 – December 31, 2023" on NERC Depreciation Expense tab of **EXHIBIT_NERC_1**.

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

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
Fax: (502) 560-5377
kglass@stites.com

Kenneth J. Gish, Jr.
STITES & HARBISON PLLC
250 West Main Street, Suite 2300
Lexington, Kentucky 40507-1758
Telephone: (859) 226-2300
Fax: (859) 253-9144
kgish@stites.com

COUNSEL FOR KENTUCKY POWER COMPANY