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

2024 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 2024, 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 SITCS38701 – Cyber – Outbound Decryption - This project is to purchase and implement an F5 Orchestrator and other F5 equipment such as Transceivers at AEP's 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 (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 (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. 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 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 Infrastructure Access Repository (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. (Closed)

- 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) that 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. (Closed)

- 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. (Closed)

- W/O SITCU51101 – Cyber-SCM-CognoseCIPRpting - Using COGNOS, integrations will be built from 20+ technology and 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. (Closed)

- 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). (Closed)

- 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 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 do not deviate from the approved standard. (Closed)

- 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 solution's 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. (Closed)

- 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). (Closed)

- 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. (Closed)

- W/O SITCX26401 – Cyber-Training Optimization – Development of newly required compliance training modules that will be uploaded to Workday for security, technology, and NERC CIP compliance requirements. Design and development and content creation. (Open)

- W/O SITCX28001 – Cyber-Axonius Sec Ast Mgmt – This tool will ensure a total asset coverage view, necessary asset data elements, holistic asset reporting, and the ability to support network vulnerability remediation work. This is a solution that detects all assets via automation, even if they do not have a vulnerability, to ensure that all assets are managed and have appropriate protections in place. (Open)

The Company completed work and closed out 12 of the projects listed above over the course of 2024. Eight 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 ($1,358,655)[1] and carrying charge ($393,074)[2] amounts incurred between the end of the test year in Case No. 2023-00159 (March 31, 2023) and the end of calendar year 2024 is $1,751,729. The support for the deferred depreciation expense calculation is shown on **EXHIBIT NERC-1**. The support for the calculation of the deferred carrying charge is shown on **EXHIBIT NERC-2**. No operation and maintenance expense was incurred related to these projects.

[1] See "Depreciation Expense for period April 1,2023 – December 31, 2024" on NERC Depreciation Expense tab of **EXHIBIT_NERC_1**.
[2] See "Total CC April 1, 2023 – December 31, 2024" on CC on investment tab of **EXHIBIT_NERC_2**.

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