COMMONWEALTH OF KENTUCKY

BEFORE THE PUBLIC SERVICE COMMISSION

In the Matter of:

ELECTRONIC APPLICATION OF KENTUCKY UTILITIES COMPANY FOR AN ADJUSTMENT OF ITS ELECTRIC RATES AND APPROVAL OF CERTAIN REGULATORY AND ACCOUNTING TREATMENTS	**)**	**CASE NO. 2025-00113**

In the Matter of:

ELECTRONIC APPLICATION OF LOUISVILLE GAS AND ELECTRIC COMPANY FOR AN ADJUSTMENT OF ITS ELECTRIC AND GAS RATES, AND APPROVAL OF CERTAIN REGULATORY AND ACCOUNTING TREATMENTS	**)**	**CASE NO. 2025-00114**

DIRECT TESTIMONY OF
DANIEL JOHNSON
SENIOR VICE PRESIDENT, CHIEF INFORMATION OFFICER
FOR PPL SERVICES CORPORATION
ON BEHALF OF
KENTUCKY UTILITIES COMPANY AND
LOUISVILLE GAS AND ELECTRIC COMPANY

Filed: May 30, 2025

TABLE OF CONTENTS

INTRODUCTION

Q. Please state your name, position, and business address.

A. My name is Daniel Johnson. I am Senior Vice President, Chief Information Officer for PPL Services Corporation ("PPL"), which provides services to Kentucky Utilities Company ("KU") and Louisville Gas and Electric Company ("LG&E") (collectively, "Companies"). My business address is 280 Melrose Street, Providence, Rhode Island 02907. A complete statement of my education and work experience is attached to this testimony as Appendix A.

Q. What is the purpose of your direct testimony?

A. I will report on the current state of PPL and the Companies' information technology ("IT") infrastructure, discuss the significant need for upgrades to modernize and streamline this infrastructure, and to provide context on these plans to support the Companies' applications for an increase in their electric and gas (LG&E only) base rates. I will report on the state of the Companies' customer-facing, business-facing, operations, and cybersecurity IT systems, as well as the Companies' multi-year assessment of the operational risks of the current systems. I will explain why investment in upgrades to IT systems is necessary to secure critical infrastructure against cybersecurity threats, stabilize IT infrastructure, streamline customer service and billing processes, ensure cost-efficiency across all systems, and better evaluate and leverage new technologies in the future.

Q. Are you sponsoring any exhibits?

A. Yes, I am sponsoring the following exhibits:

Exhibit DJ-1 CONFIDENTIAL Cybersecurity Risks

IT INFRASTRUCTURE OVERVIEW, RISKS, AND SYSTEMS

Q. Please describe the role of IT Infrastructure in the Companies' operations.

A. The Companies' IT infrastructure is essential to every part of their operations. Operating an efficient, modern utility means storing, processing, and utilizing large quantities of data every single day. In the past, the number of employees that were directly accessing and working with the Companies' IT was limited. However, in an interconnected, modern utility, nearly everyone relies on dependable IT systems to do their jobs. Whether they are linemen, generation unit engineers, accountants, or customer service personnel, the Companies' employees constantly transmit and receive information and important communications through the Companies' shared platforms. To continue to deliver reliable and reasonably priced electricity and gas to customers, the Companies must ensure that this information is safe from predatory outside groups, maintained on a stable platform, and efficiently organized so it can be used effectively.

Q. Describe how the IT landscape has changed since the Companies' 2020 rate cases and the challenges presented by those changes.

A. As with the rest of the business world, over the past five years since COVID the Companies have achieved significant operating efficiencies via remote meetings, file-sharing systems, and other mainstream workflow software. But evolution of technology has also introduced new and complex challenges to the Companies' IT operations. These challenges include rapid growth of new technologies associated with demand side management ("DSM") programs, industrial-scale behind-the-meter generation operations, and advanced metering infrastructure ("AMI"). These advancements have added new complexity to what was previously a simpler, one directional movement of energy to customers. To meet the challenges presented by

this complexity, now more than ever, accessing understandable, useful real-time information is critical to effective operations.

There are also new expectations for customer service. The electrification of vehicles and homes has made customers more conscious of their energy bills. This has led to customer demand for transparent, accessible information about their bills and energy usage so that customers can maximize their savings. As customer needs continue to evolve, it is likely that the Companies will become even more dependent on an efficient, stable IT infrastructure to meet these new expectations.

Most importantly, the Companies' IT infrastructure is more essential than ever to keeping its operations secure. The Companies are responsible for both critical energy infrastructure and vast amounts of highly sensitive customer, business, and contractor information, all of which is subject to threats by hostile actors. These hostile groups are constantly adopting new tactics, so outdated security systems or unwary staff can create a significant risk that critical information and systems will be compromised. The rapid evolution of AI has made these attacks even more effective and frequent.

Q. Describe the Companies' Current IT Infrastructure.

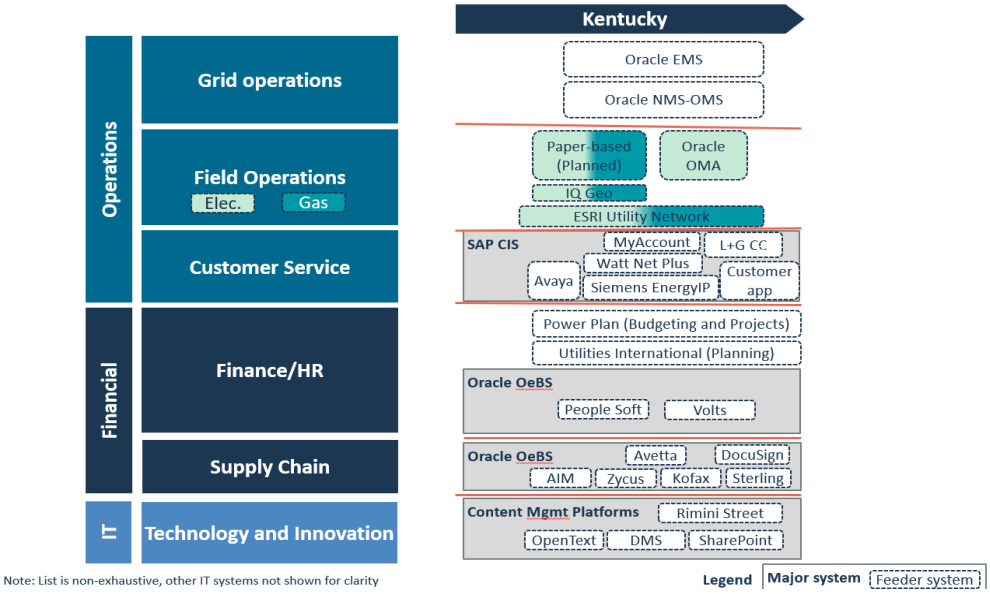
A. The Companies' current IT infrastructure consists of an array of interconnected platforms that fall into a handful of categories: Field operations, cybersecurity, business-side IT (often called enterprise resource planning, or "ERP"), customer side IT, and content management platforms. Many of these components are currently run "on premise" using the Companies' own hardware. Current software applications include:

- **Field Operations:** The Companies' field operations rely on CGI's OpenGrid, which is a widely used system for infrastructure management. Although this system is in part paper-based, OpenGrid still has access to vendor support with no foreseeable end-date. In addition, the Companies use Environmental Systems Research Institute, Inc.'s ("ESRI") suite of Geographic Information Systems ("GIS") tools for system mapping needs.
- **Grid Management:** The grid management systems include Network Management Systems for day-to-day operations and Emergency Management Systems in the event of unexpected events that threaten to impair grid function. These are operated using the Oracle Corporation's ("Oracle") Network Management Systems ("NMS").
- **Cybersecurity:** The Companies use an array of cybersecurity products to ensure that staff and customers are protected against unauthorized security breaches or cyberattacks, and they employ numerous staff who are dedicated to Cybersecurity on a full-time basis. The Companies also benchmark cybersecurity operations and strive to achieve target levels of maturity consistent with our peers in the industry.
- **ERP**: The Companies operate their finance and supply chain systems on the Oracle E-Business Suite ("OeBS") platform, and its human resources system uses Oracle Peoplesoft as well as an in-house time-keeping system for its field teams called Virtual Online Time Systems ("VOLTS"). OeBS was last updated in 2020 and has vendor support through 2034. Because the OeBS system does not have all of the functions needed to meet the Companies' supply-chain

system requirements, including supplier compliance and procurement management, the Companies supplement the system with additional "bolt-on" applications including Avetta (compliance) and Zycus (procurement) to fill these gaps.

- **Customer Information System ("CIS")**: The Companies began using SAP SE's ("SAP") Customer Care System ("CCS") in 2007. The Companies' SAP CCS system has full vendor support through 2027.
- **Customer Experience ("CX"):** The Companies' CX platforms – which power the channels that customers use to interact with the Companies – consist of phone-based customer support, the "MyAccount" webpage, and its mobile app. The Companies developed the "MyAccount" customer website through the SAP Utility Customer E-Services System ("UCES") platform and developed their mobile app in house. Additionally, the Companies' current contact center and Interactive Voice Response ("IVR") platform is obsolete and in need of replacement.
- **Content Management Platforms:** The Companies rely on an array of different content management platforms to share projects and information between groups and with third parties.

A visual representation of these systems is depicted in Table 1, below:



Q. Does the Companies' existing IT infrastructure position them to efficiently serve customers in the future?

A. No. While the Companies' current IT infrastructure remains capable of carrying out day-to-day functions in the near term, managing these disparate systems and maintaining aging hardware and software infrastructure requires roughly 90% of the Companies' IT resources. This leaves few IT resources remaining to identify and work on applications, systems and software that will position the Companies well to serve their customers reliably in the future.

In addition, there are barriers to sharing information across the disparate platforms within PPL, which are only overcome through manual entry, requiring time and effort from non-IT staff. In short, the Companies' current IT infrastructure could maintain the *status quo* in the near term, but is growing increasingly costly, becoming less reliable, and, ultimately, is hampering the Companies' ability to find forward thinking, more efficient ways to serve its customers. This is not a sustainable approach to managing this important part of the Companies' long-term success.

Q. What specific risks and challenges have been identified in the Companies' IT infrastructure?

A. Many systems are either aging, nearing the end of their service contracts, or reaching "end-of-life," which is the point at which an IT product is no longer maintained or supported by its manufacturer. Obsolescence is looming. For example:

- **VOLTS:** VOLTS was developed in house and therefore has no external vendor support. Maintenance of the software relies on institutional knowledge within the Companies. As employees who developed and implemented the system move on and retire, resolving issues with the system and adapting it to different needs will grow more difficult.
- **Mobile App:** The Companies' mobile app was also developed in house and interfaces with existing systems. When those systems change, the mobile app will need significant reprogramming to maintain effective interface with those systems.
- **Website**: The Companies' "MyAccount" website was developed using the SAP UCES software, which is no longer in operation. Therefore, MyAccount is considered beyond end-of-life and there is no longer vendor support for this product.
- **OeBS and PeopleSoft:** Oracle is actively working to move all of its utility customers away from on-premises OeBS platforms and towards cloud-based versions, primarily by making new data processing and analytics tools available exclusively to its cloud-based customers. As noted above, the Companies must already use an array of bolt-on applications for OeBS due to

additional functionality required by their business operations. Continuing to use on-premises OeBS means that the Companies will need to continue to spend resources modifying an outdated platform. As the cloud-based platform becomes standard, the Companies will have difficulty finding staff with experience using the on-premises version of the software.

- **Opengrid:** Some components of the Companies' OpenGrid system are 100% paper-based, and the system runs on aging software, which limits its ability to incorporate new features as they become industry standard. For example, OpenGrid lacks the ability to track information at the work order level or to track information about specific assets in real time.
- **SAP CCS System:** This system will lose mainstream support in 2027 and will no longer have access to regular updates. Unless upgraded, post-2027, the Companies would be required to enter Customer-Specific Maintenance, which introduces significant operational risks, including:
  - **No delivery of legal changes**, potentially impacting regulatory compliance.
  - **No support packages or guaranteed technological updates**, limiting system compatibility with new database and operating system versions.
  - **No direct upgrade paths**, leading to complex multi-step migrations in the future.
  - **No new system patches,** reducing SAP supported issue resolution and increasing customization.
  - **Limited interface support**, increasing potential integration failures.

- **Degraded support service levels**, including loss of guaranteed response times and remote support.
- **Increased cost exposure**, as the burden of resolving new system issues shifts to the Companies.

Given the critical role of CCS in billing and financial operations, this level of risk is unacceptable.

As these platforms lose vendor support and vendors move towards offering cloud-based services, the Companies' IT infrastructure – which is not well suited for a migration to cloud based services – will likely require bespoke, fit-for-purpose software patches and fixes to maintain the existing systems.

Q. Do the Companies' IT infrastructure challenges affect the cost of providing utility service?

A. Yes. As stated above, the majority of the Companies' IT resources are spent keeping systems running – fixing hardware, patching software errors, and keeping the IT infrastructure stable so that the Companies can carry out their day-to-day obligation to provide service. The cost-burden that this places on our customers is two-fold.

First, as these systems continue to age and lose support resources, the Companies will be forced to invest more to keep its infrastructure at an acceptable level of efficiency, safety, and reliability. These necessary expenses will eventually be borne by customers, leading to higher rates with no consequent improvements for the customers.

Second, making capital investments in maintaining these aging and inflexible IT systems stunts innovation and improvement. Focusing the efforts of the Companies'

IT personnel on keeping day-to-day operations running prevents the Companies from taking a long-term view of its IT operations. If the Companies' IT staff is solely dedicated to the day-to-day, they cannot evaluate new ways to leverage IT systems and new processes to improve customer experience, streamline operations-side efficiency, and allow the Companies to most effectively use their resources to serve their customers.

PLANNED IT UPGRADES

Q. How do the Companies plan to address the challenges you have identified in your testimony?

A. The Companies have developed a five-year plan to overhaul their aging IT infrastructure, reorient the Companies' IT expenditures towards improving their IT operations, and develop an understanding of how to use emerging technologies to effectively improve their operations. The plan was created as part of PPL's efforts to operate more efficiently by improving cooperation and information sharing across its jurisdictional utilities. Beginning in 2023, PPL determined that it needed to better align the IT systems maintained by different utilities within the organization and to identify and study weaknesses and risks in the IT infrastructures of each utility.

Q. What was the scope of that review?

A. PPL examined the systems supporting the field, grid, customer service, ERP, and data management operations of its different jurisdictional utilities. In all, these systems account for between 50-60% of all IT expenditures across PPL.

Q. What were the findings of PPL's review?

A. Overall, the review confirmed what PPL had already suspected – that the lack of a consolidated organizational platform created inefficiencies for the organization. The

review also identified numerous risks stemming from the age, complexity, and inflexibility of its current IT infrastructure. Overall, PPL concluded that a number of the utilities' systems were not meeting the needs of its customers or employees, and were hindering the Companies' efforts to operate efficiently, share ideas with PPL's other jurisdictional utilities, and adapt to new challenges.

Q. Please provide some examples of the issues the IT infrastructure was experiencing.

A. The comprehensive IT systems review identified the following issues for example:

- More frequent than desired outages to high and middle priority IT systems.
- Few apps and systems running on the cloud.
- Low rates of resolution for help tickets handled by automated systems with no human intervention.
- Proliferation of applications across operating utilities, many performing similar functions, and lack of integration of those systems at the PPL level.
- Higher levels of expenditure on hardware maintenance and software patching than on preventative maintenance.
- Many systems at or near obsolescence risk, with as many as 10% of the operating systems, 32% of storage systems, and 52% of the network switches reaching end of life at or before 2025.

Q. How has PPL responded to the findings of its IT systems review?

A. PPL determined that in addition to immediate repairs to stabilize and secure its IT infrastructure, PPL and the Companies must make strategic changes to how they manage and maintain IT infrastructure. In 2024, therefore, PPL launched a targeted

and strategic plan to consolidate its systems, overhaul its processes, and become more flexible to future changes in IT.

Q. Please explain PPL's plan to upgrade IT systems.

A. PPL organized its plan around a number of different "value streams" – which are simply categories of solutions and people who build those solutions for a broader business objective. The value streams included in the plan are: (1) Advanced Customer Operations and Engagement, which includes CIS and customer experience platforms and metering modernization; (2) Predictive Field Operations and Asset Management, which includes Work and Asset Management Consolidation; (3) Grid and Pipeline of the Future, which includes unified GIS and intelligent grid operations across all utilities; (4) Next Generation or "NextGen" Enterprise Services, which includes human resources solutions and corporate and financial enterprise solutions; (5) Data analytics and AI; (6) Cybersecurity; and (7) Infrastructure and Other.

Across all value streams, PPL's plan further includes three overlapping phases: Run, Grow, and Transform. The "Run" phase of plan is focused on stabilizing and securing PPL's day-to-day operations by replacing obsolete hardware and software systems. During this phase, PPL will also free up its IT resources for more proactive projects by contracting these more basic IT support operations to a managed services company. The "Grow" phase will focus on preparing PPL's different utilities and employees to implement a more cohesive and efficient IT infrastructure. Finally, the "Transform" phase of the plan will focus on bringing the PPL's IT systems and capabilities into the future.

RUN PHASE

Q. How will day-to-day operations change during the "Run" phase?

A. The Run phase of the IT upgrade strategy, which began in early April 2025, focuses on making changes that will meet the immediate needs of the Companies' employees and customers while freeing up resources to carry out PPL's long term IT goals. This is expected to produce short-term improvements by reducing the number of recurring IT incidents, increasing the number of issues resolved through automated fixes, reducing backlogs, and adding new and improved security services.

Q. How does PPL plan to free up IT employees to focus on long term goals?

A. PPL has entered into a managed services agreement ("Managed Services Agreement") with a vendor to manage and stabilize PPL's day-to-day IT and cybersecurity operations.

Q. What services are included as part of the Managed Services Agreement?

A. The Managed Services Agreement covers three primary IT functions previously performed by PPL employees: (1) application managed services; (2) managed security services; and (3) infrastructure managed services. By transferring these functions to an outside vendor, PPL expects to reduce IT operations risk, reduce duplication of applications and systems, increase automation, and add new and improved IT security services, making the Companies' systems more secure and more efficient.

Q. How will the Managed Services Agreement create cost-savings?

A. The Managed Services Agreement includes a commitment by the vendor to reduce PPL's IT operations costs for functions within the scope of the MSA by 50% over a five-year span. In addition, the vendor has agreed to partner with PPL to share in the costs to transition to the managed services structure.

Q. How will the Managed Services Agreement enable PPL to focus on its long-term IT goals?

A. By transferring employee time devoted to day-to-day operations and cutting IT operation costs, the Managed Services Agreement will free up PPL employee capacity for investment in skills training as well as identifying and implementing its new consolidated platforms.

GROW PHASE

Q. Why does the IT upgrade plan contain a "Grow" phase?

A. The Grow phase is intended to make sure that the correct IT policies, organizational structures, and talent are in place before PPL makes extensive investments in new operations.

Q. Describe the policies that PPL will implement to ensure that the upgrades to IT systems are cost effective.

A. To use new IT systems to meaningfully improve its operations, PPL will maximize the value the new systems can bring, measure that value, and ensure that employees are positioned to take advantage of value-added systems. To that end, the Grow phase will implement the following policies:

- **Modernize IT Financial Management:** IT Financial Management is a way for companies to track the financial performance of their IT infrastructure. By adopting tools and identifying metrics that will track the performance of its IT systems in real time, PPL will be better able to evaluate the state of its IT infrastructure and the actual benefits produced by different IT system changes.

- **Scaled Agile Framework (SAFe):** PPL will train its employees to implement the SAFe approach. SAFe relies on groups of employees from across different operations teams and prioritizes flexible decision making, collaboration, and solutions that best serve PPL's end-goal. PPL will implement SAFe training for its business, IT, and Field Operations Teams, alongside more conventional IT skills development.
- **Value Realization Office:** The creation of a Value Realization Office, with a staff of individuals dedicated to overseeing the IT upgrades, tracking and reporting the effectiveness of different parts of the plan, and assisting operations teams in implementing these new systems.
- **Assessment and preparation for new programs:** PPL is undertaking an organization wide assessment of its work efficiency and determining the best way to incorporate new IT systems to make its operations more efficient and effective.
- **Skills development:** PPL is investing in training its employees to adjust to working with the new, consolidated platforms and managed services arrangements, learning how SAFe will function, and implementing uniform cybersecurity best practices.
- **Data & AI:** PPL is actively recruiting individuals who have a background in data analytics and AI to build a team that will be able to determine how to implement new machine learning and AI technologies in a way that actually improves operations.

Q. When will these policies be implemented?

A. While implementing these policies and programs will be an ongoing project, the majority of these policies and organizational changes will be fully adopted by the middle of 2027. Programs such as building up the capabilities of the Data & AI value stream and identifying automation efficiencies are expected to be ongoing throughout the implementation of IT upgrades.

TRANSFORM PHASE

Q. Describe the Transform phase of PPL's plan to upgrade IT systems.

A. The Transform phase is the implementation of PPL's selected next-generation IT systems through different value streams, and the creation of a Data and AI team within IT dedicated to studying advancements in and possible uses for AI and other emerging technologies.

Q. Will PPL implement all of these IT changes simultaneously?

A. No. PPL will roll out changes to the Companies' platforms over time, beginning with its CIS and ERP operations.

Q. Has PPL determined which platforms it will use for its CIS and ERP platforms?

A. Yes. PPL has chosen to implement SAP's cloud-based systems as its "wall-to-wall" CIS and ERP platforms.

Q. How did the Companies select the SAP platform?

A. PPL issued a request for quotes ("RFQ") to qualified vendors that have experience in the utility industry and have the capabilities necessary to meet current and future needs. PPL then reviewed and evaluated the responses to the RFQ using standardized criteria.

Q. What CIS and CX needs did PPL identify?

A. PPL determined that adequate CIS and CX platforms deployed across all jurisdictional utilities would need the following:

- **Billing:** PPL billing involves multiple rate structures, such as time-of-use, time-variable (real-time pricing), demand-based, and tiered pricing. The CIS platform must support these complex billing models, ensuring that customers are billed accurately. The system should also handle billing for both electric and gas. In addition, automated billing, payment processing through various channels (online, mobile, paper), and integration with financial institutions are critical.
- **AMI & Smart Grid Integration:** The CIS platform must be able to integrate with AMI and AMR technologies. This integration allows for real-time data collection and analysis, supporting load forecasting, outage management, and efficient resource allocation. Processing these large datasets and generating useful recommendations will help the Companies maintain grid reliability.
- **Customer Self-Service:** Modern customers expect transparency and control over their utility accounts. PPL's next CX platforms must include intuitive web and mobile self-service portals where customers can view usage data, make payments, and report issues. The systems should also use different communications channels – such as e-mail and SMS text messages– to ensure that customers receive timely notifications about outages, billing updates, and other critical information.
- **Automated Regulatory Reporting:** Given the regulatory landscape, the CIS must facilitate automated reporting to various oversight agencies. An effective regulatory reporting system should provide secure data management, audit trails, and features that help the utility maintain compliance with state and

federal regulations. This not only minimizes legal risks but also builds trust with customers and regulators alike.

Q. What risks are managed or mitigated by the implementation of a new CIS?

A. Moving forward with one modern CIS system will address a number of key risks, most importantly, cybersecurity and obsolescence risks with the Companies' current systems. A modern, integrated CIS will enable consistent and centralized security procedures across PPL's operating companies as opposed to the inconsistent approvals and versions they currently work in. And as I noted previously, SAP has announced that mainstream maintenance and support of the current SAP CCS applications will end on December 31, 2027. Upgrading reduces the significant and unacceptable obsolescence risks I identified earlier, given the criticality of the CIS.

Q. What are the expected capital costs to the Companies for the Advanced Customer Operations and Engagement projects?

A. As I noted earlier in my testimony, CIS and CX are considered along with other system upgrades and enhancements as a suite of solutions in a value stream called "Advanced Customer Operations and Engagement." LG&E expects to spend $43.8 million in capital on this suite of solutions, including CIS and CX, through the end of the forecast test period, with total investment over the 5-year business planning horizon of $87.7 million. KU expects to spend roughly $39 million on this value stream through the forecast test year, with total investment over the 5-year business planning horizon of approximately $78 million.

Q. What ERP needs did PPL identify?

A. PPL determined that an adequate ERP system would need the following:

- **Financial Management**: An ideal financial management system would enable accounting and budgeting to occur at the same level of detail. The ERP system must support utility-specific financial management functions, including budget and forecasting, as well as multi-entity financial consolidation. Accurate financial reporting and regulatory compliance are essential for ensuring transparency and stakeholder confidence.
- **Asset and Supply Chain Management:** An ERP platform must offer asset management features for full lifecycle of an asset. This includes an asset's procurement, maintenance, maintenance scheduling, and eventual replacement planning. Effective supply chain management is vital to ensure that parts and equipment are available at all of these stages.
- **Human Capital Management ("HCM"):** An ERP system that incorporates human capital management can streamline workforce scheduling, payroll processing, and compliance with labor regulations. This is especially important for managing the Companies' crucial Field Operations. An effective HCM module ensures that the right personnel are available to handle operational tasks.
- **Business Intelligence and Analytics:** PPL's next ERP platform should include analytics capabilities that track key performance indicators (KPIs), predict maintenance needs through AI, and support long-term thinking.

Q. Did PPL consider any other factors in selecting a platform?

A. Yes. In addition to these criteria, PPL evaluated the platforms based on their ability to integrate with other systems, vendor support, adaptability to new conditions such as

regulatory requirements, and total cost. Additionally, PPL determined that a cloud-based platform was optimal due to overall advantages in support, reduced overhead, and cyber-security support. For example, many vendors are investing in new capabilities and features for cloud-supported products that are not available for legacy on-premise systems. Cloud-based systems are also advantageous in that system updates are automatically pushed to customers, eliminating the need for scheduling and implementation of updates, some of which may be critical to system security. Cloud-hosted products also offer additional business continuity and disaster recovery capabilities by increasing redundancy and decreasing the costs of conducting disaster recovery testing. Cloud providers offer multiple data centers and include redundant infrastructure to enable secure data storage. This redundancy protects against significant downtime or failure of infrastructure. Cloud-hosted products also decrease dependence on internal resources for disaster recovery testing and planning.

Q. When will PPL and the Companies' implement the new systems?

A. We plan to fully implement the SAP platform for ERP operations by 2027 and for CIS operations by the end of 2028.

Q. What are the expected capital costs to the Companies for the planned upgrades to the ERP and other NextGen Enterprise Services?

A. For the NextGen Enterprise Services value stream, which includes ERP but also standard enterprise-level projects, LG&E expects to spend approximately $27.4 million in capital for strategic projects through the forecast test period, with total investment over the 5-year business planning horizon of approximately $31 million. KU expects to spend roughly $24.3 million on this value stream for strategic projects through the

forecast test year, with total investment over the 5-year business planning horizon of approximately $27.2 million.

Q. What other IT infrastructure improvements will the Companies' implement?

A. Over time, all PPL utilities, including the Companies, will implement additional changes to customer service interfaces and across grid and field operations. On the Customer side, the Companies plan to create more integrated customer experience ("CX") platforms that better facilitate self-service for customers and allow them to switch seamlessly between phone, mobile app, and web or electronic communications with the Company. This will include upgrades to the current IVR systems.

For field operations, the Companies plan to implement updated systems that will modernize field-time entry, enable real-time field information sharing by its employees, and will examine the use of predictive technologies to improve vegetation management. Finally, the Companies' grid and pipeline operations plan to unify their GIS systems with PPL's other jurisdictional utilities, use predictive weather models to better assess system risks, and employ the use of drones for asset inspections.

Q. Have PPL and the Companies determined what systems they will use to implement these improvements?

A. Not yet, but we are nearing final selection of some systems that will serve the functions described above. We are continuously monitoring industry implementation of technological improvements and – as with the ERP and CIS platforms – determine the criteria for selecting the right systems.

Q. What are the expected capital costs to the Companies for the planned upgrades to IT systems to support Grid & Pipeline and Field Operations and Asset Management?

A. For the Grid and Pipeline of the Future value stream, LG&E expects to spend approximately $9 million in capital for strategic projects through the forecast test period, with total investment over the 5-year business planning horizon of approximately $15 million. KU expects to spend roughly $17.5 million on this value stream for strategic projects through the forecast test year, with total investment over the 5-year business planning horizon of approximately $22.8 million. For the Field Operations and Asset Management value stream, LG&E expects to spend approximately $12.2 million in capital for strategic projects through the forecast test period, with the investments completed by the end of 2026. KU expects to spend roughly $10.9 million on this value stream for strategic projects through the forecast test year.

Q. How do you plan to manage reliability risks from implementing new technologies?

A. Given the critical role that the Companies serve and the importance of IT systems in supporting that role, careful evaluation of emerging technologies is even more important. The goal of the Transform initiative is not to place PPL or the Companies on the bleeding edge of technological advancement – it is to carry out long-term, thoughtful assessments and implementations of emerging technologies and their use cases. By thinking about transformative technologies early and carefully, we will be positioned to implement any technological innovations in a way that makes financial and practical sense for the Companies and their customers.

Q. How will AI be utilized in the Transform phase of the upgrade plan?

A. Developments in AI include promising technologies that may revolutionize grid-management, cybersecurity, customer engagement, and data processing. If these technologies live up to their billing, the potential benefits to customers in the form of savings and operational efficiency will be significant. However, PPL's and the Companies' top priority remains the safe and reliable delivery of energy to customers, and there are still serious questions about these technologies that must be resolved before they can be relied on in sensitive parts of operations.[1] Therefore, PPL and the Companies are committed to closely studying industry use-cases to determine where AI can create efficiencies, and where it creates unacceptable risks.

Q. Are there any areas where PPL and the Companies expect to implement AI?

A. Yes. We believe that there are ways to immediately free up resources using AI and other automation systems to carry out low-level, time-consuming, and repetitive tasks. These include cataloguing incidents, maintaining data sets and processing data to generate reports, managing login credentials and user access, and fixing and patching routine IT problems. In addition, the Data & AI team will use AI to examine asset planning and look for other organization wide efficiencies.

CYBERSECURITY

Q. What is the primary goal of the Companies' cybersecurity operations?

[1] *See DOE Delivers Initial Risk Assessment on Artificial Intelligence for Critical Energy Infrastructure*, DOE (Apr. 29, 2024), https://www.energy.gov/ceser/articles/doe-delivers-initial-risk-assessment-artificial-intelligence-critical-energy.

A. The primary goal of the Companies' cybersecurity operations is to protect critical infrastructure, which includes grid operations and the operational technologies and the IT systems that keep these operations running.

Q. What is the current state of the cybersecurity landscape for utilities?

A. Like the rest of its business operations, the current cybersecurity landscape for utilities has been complicated by new technologies such as interconnected management systems and smart grid systems. These interconnected technologies produce new layers of sensitive data containing customer and business information such as personal data, usage information, time of use information, and other information that can be exploited by savvy threat actors. Utilities in general are susceptible to cyberattacks due to their broad geographic footprint and the number of "smart" devices deployed in the field and the interdependence between those devices and the software required to make them valuable.[2] They are also targets for sophisticated cyber criminals and nation-states because of the potential scope of disruption that can be caused by a successful cyberattack.

In short, cybersecurity incidents pose tremendous risks to utilities and their customers and have the potential to result in disruption of energy delivery, destruction of physical and cyber assets, exposure of sensitive business and customer data, and disruption of day-to-day business operations, among other risks.

Q. What common cybersecurity threats do the Companies experience?

A. The Companies are generally faced with two major forms of cybersecurity threats. Computerized attacks, such as malware and ransomware, are designed to exploit

[2] *E.g.*, The energy sector threat: How to address cybersecurity vulnerabilities | McKinsey.

vulnerabilities in the Companies' IT systems to extract information or halt operations. Social engineering attacks, such as phishing, attempt to deceive employees or others with access to sensitive information or system access information into revealing that information to gain unauthorized access to systems. These two types of threats are often used together – for example, a social engineering attacker may include malware in a document, or a computerized attack may have been set up by obtaining sensitive information about IT systems through social engineering.

Q. Please explain how cybersecurity strategy has evolved to combat these new threats.

A. In the past, utilities typically viewed cybersecurity as a one-time investment – vendors sold technology that met perceived threats, utilities purchased these solutions, and they then updated them as needed. Today, cybersecurity requires continuous attention, maintenance, employee training, and updates. Given the Companies' reliance on their IT infrastructure to run their critical infrastructure, cybersecurity is now a central focus of our security operations, and a regular topic of discussion for all of our operations.

Q. Does the current IT infrastructure contain vulnerabilities that could be exploited by threat actors?

A. Yes. Certain potential vulnerabilities were identified in PPL's overall review of its systems and they are summarized in **Exhibit DJ-1** to my testimony, which is designated as **CONFIDENTIAL** due to the potentially sensitive nature of the findings. Many of the identified issues stem from the absence of a consolidated IT infrastructure with standardized processes and information access policies. As long as the Companies

maintain different systems across operating companies, many of these vulnerabilities will continue to exist.

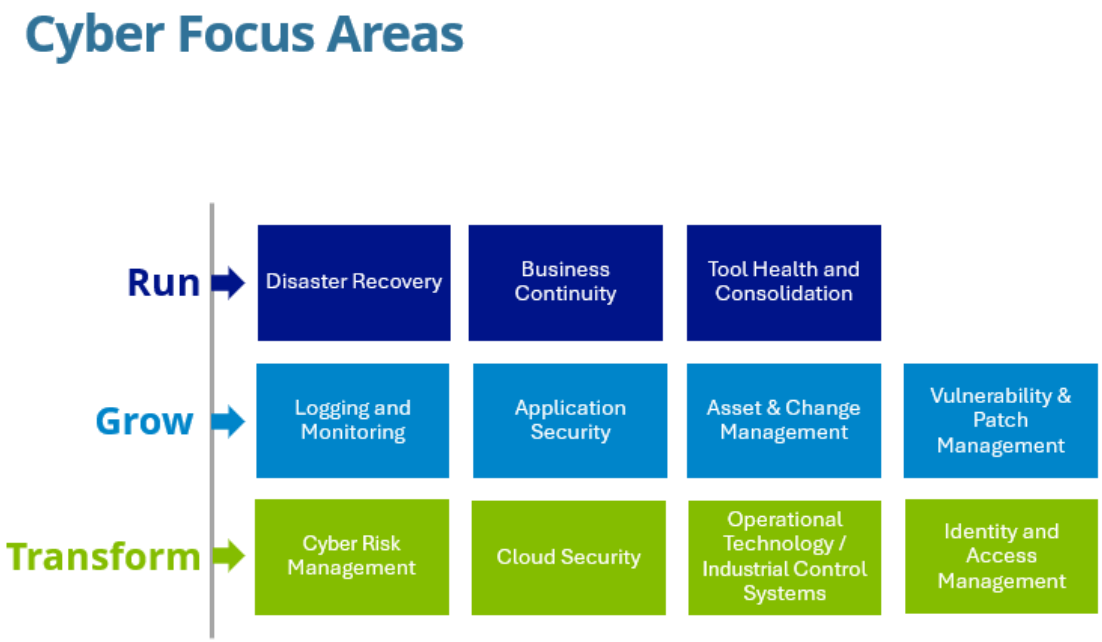
Q. Will the planned IT upgrades address these vulnerabilities?

A. Yes. Overall, the planned upgrades will improve cybersecurity across the PPL utilities by consolidating all IT systems, which will mitigate many of the risks identified in Exhibit DJ-1. In addition, PPL will reassess and strengthen different parts of cybersecurity infrastructure during each stage of the upgrade plan.

Q. Please explain how the different phases of the planned upgrades will support the Companies' cybersecurity infrastructure.

A. The "Run," "Grow," and "Transform" phases of the upgrade plan will support the Companies' cybersecurity infrastructure. In the "Run" phase, through its managed services agreement, the Companies will solidify their recovery planning operations, which will ensure that in the event of an incident the Companies will be capable of restoring their systems. The Companies will also assess the different cybersecurity tools in use and consolidate them into one modern cybersecurity toolkit. As the upgrade plan moves into the "Grow" phase, we will assess application security, develop better protocols for vulnerability management and threat monitoring, and invest in cybersecurity skills training for employees. These are intended as organization wide preparations to make it easier to implement future cybersecurity programs. In the "Transform" phase, once a set of uniform protocols and systems is in place, our cybersecurity operations will implement advanced cybersecurity risk management, cloud security programs, more advanced identity and access management systems, and

investments in specialized staff to secure the Companies' operational technology. A visual depiction of the plan is included below:



Q Does the Managed Services Agreement include cybersecurity protection?

A. Yes. Although PPL and the Companies plan to maintain their own technology security team, the Managed Services Agreement will help the Companies with additional cybersecurity resources for 24x7 security monitoring and detection, along with disaster recovery and business continuity operations when faced with cybersecurity threats or incidents.

Q. What are the expected capital costs to the Companies for the planned upgrades to the Cybersecurity value stream?

A. LG&E expects to spend close to $5.9 million in capital for strategic cybersecurity initiatives through the forecast test year. However, once the systems and processes described in my testimony are fully implemented, the capital costs for cybersecurity

are expected to decrease, with a total of $8.6 million for cybersecurity strategic initiatives over the 5-year planning period through 2029.

KU expects to spend roughly $5.3 million in capital on cybersecurity strategic initiatives through the forecast test year. But as with LG&E, capital expenses for KU cybersecurity strategic initiatives are expected to decrease after 2026, with a total capital spend of approximately $7.8 million through 2029.

COST SAVINGS

Q. Will the planned IT upgrades create quantifiable benefits for the Companies' customers?

A. Yes. While the primary motive for the upgrades is the long-term security and stability of IT systems and the Companies' critical infrastructure, they will also create long-term benefits for the Companies' customers both in the form of cost-savings and improved customer services. Ms. Montgomery summarizes the customer-services benefits of the upgrades in more detail in her testimony, but they include new and enhanced self-service options for customers that will operate across integrated platforms, and ability for customers to begin interactions on one device and continue on another device.

Q. How will the upgrades drive operational efficiencies that will benefit customers?

A. The upgrades will generate efficiencies which will benefit customers in the form of lower operations and maintenance costs for the Companies' IT operations. Specifically, the upgrades are expected to achieve the following cost and operational efficiencies, among others: (1) reduced costs for support and licensing of multiple systems and efficiencies through centralized support at the PPL level; (2) streamlined implementation of new system functionality across all operating companies, including potential implementation of AI advancements; (3) reduction in manual data

reconciliation and data collection to support enterprise-wide insights and analysis; (4) billing and process automations and handling time efficiencies for customer services operations; (5) reduction in clerical, engineering, and scheduler manual administrative work to support field operations; and (6) overall reduction in system maintenance and manual process for enterprise services.

Thus, not only will customers benefit from the risk reduction to the Companies' IT operations, they will also benefit from substantial operational efficiencies created across all value streams.

CONCLUSION

Q. Does this conclude your testimony?

A. Yes, it does.

VERIFICATION

STATE OF RHODE ISLAND)
)
COUNTY OF Providence)

The undersigned, **Daniel J. Johnson**, being duly sworn, deposes and says that he is Senior Vice President and Chief Information Officer for PPL Services Corporation and he provides services to Louisville Gas and Electric Company and Kentucky Utilities Company, that he has personal knowledge of the matters set forth in the foregoing testimony, and that the answers contained therein are true and correct to the best of his information, knowledge, and belief.

Daniel J. Johnson

Daniel J. Johnson

Subscribed and sworn to before me, a Notary Public in and before said County and State, this 29th day of May, 2025.

Danielle Balzan

Notary Public

Notary Public, ID No. 01BA8383644
(SEAL)

My Commission Expires: 8/21/2025

DANIELLE BALZAN
NOTARY PUBLIC, STATE OF NEW YORK
Registration No. 01BA6383644
Qualified in Albany County
Commission Expires August 21,2025

APPENDIX A

Daniel Johnson
Senior Vice President, Chief Information Officer
PPL Services Corporation
280 Melrose Street
Providence, RI 02907

Professional Experience

PPL Services Corporation	
Senior Vice President, Chief Information Officer	2024 - Present
Guardian Life	
Chief Technology Officer and Head of Technology	2013 - 2024
NBC Universal/Comcast	
Chief Technology Officer and Senior Vice President	2007 - 2013
Vice President, Technology Governance	2004 - 2007
General Electric (GE)	
Client CIO, Business Solutions	2000 - 2004

Professional Memberships

Member, NPower National Advisory Council (Creates pathways to economic prosperity by launching digital careers for military veterans and young adults from underserved communities.)

Civic Activities

President, Bethlehem Lacrosse Club (a 501c3 organization that provides an enjoyable development experience with the program while learning lacrosse for boys and girls from kindergarten to 6th grade.)

Education

Double Master of Business Administration (MBA) Information Systems and Finance
Fordham University, New York, NY

Bachelor of Science, Management Information Systems (MIS)
LeMoyne College, Syracuse, NY