EXH. BEF-1CT
DOCKETS UE-240004/UG-240005
2024 PSE GENERAL RATE CASE
WITNESS: BRIAN E. FELLON

BEFORE THE
WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION, **Complainant,** **v.** **PUGET SOUND ENERGY,** **Respondent.**	**Docket UE-240004** **Docket UG-240005**

PREFILED DIRECT TESTIMONY (CONFIDENTIAL) OF

BRIAN E. FELLON

ON BEHALF OF PUGET SOUND ENERGY

REDACTED VERSION

FEBRUARY 15, 2024

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (CONFIDENTIAL) OF BRIAN E. FELLON

CONTENTS

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (CONFIDENTIAL) OF BRIAN E. FELLON

LIST OF EXHIBITS

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (CONFIDENTIAL) OF BRIAN E. FELLON

I. INTRODUCTION

Q. Please state your name, business address, and position with Puget Sound Energy.

A. My name is Brian Fellon, and my business address is P.O. Box 97034, Bellevue, Washington 98009-9734. I am the Director of Information Technology ("IT") Application Services for Puget Sound Energy ("PSE" or the "Company").

Q. Have you prepared an exhibit describing your education, relevant employment experience, and other professional qualifications?

A. Yes, I have. It is Exh. BEF-2.

Q. What are your duties as Director of Information Technology Application Services?

A. I am responsible for the full lifecycle of software applications at PSE, including development, delivery, support, architecture, and project management.

Q. What topics are you covering in your testimony?

A. First, my testimony provides an overview of PSE's IT vision and strategy and demonstrates how PSE's proposed investment plan presented in this case supports PSE's clean energy transformation, its corporate commitments to safety and

reliability, and delivery of PSE's IT strategy. My testimony addresses key risks and challenges associated with PSE's proposed investment plan as it relates to the delivery of PSE's IT strategy. As part of this, I explain the critical role IT plays in supporting PSE's clean energy objectives, why IT modernization programs are necessary to improve technology reliability, security and overall resiliency of critical PSE systems, and to enhance the customer experience.

Second, my testimony describes how most of PSE IT investments are identified and approved, including both program and project related investments. PSE defines a "project" as a temporary endeavor undertaken to create a unique service or result. Projects are temporary and close upon completion of the work they were chartered to deliver. In contrast, PSE defines a "program" as the coordinated organization, direction, and implementation of a collection of related projects and complex activities, driven by strategic goals or importance, which when executed together, achieve outcomes and benefits not available from managing them individually. My testimony explains how technology solutions are designed for each program or project, the procurement process for new technology solutions, and how technology programs and projects are governed.

Finally, my testimony provides a description of the technology investments PSE seeks recovery for in this case, broken out into investments projected to be placed in service January 1, 2025, through December 31, 2026. As part of this, I also provide details on any major IT programs or projects included in PSE's cost recovery request that are expected to cost more than $15 million.

Q. Will your testimony cover all IT investments PSE is requesting recovery for in this case?

A. PSE's IT investments are categorized into three major strategic work streams:

- Business Enablement
- Systems Modernization
- Strategic Initiatives

My testimony covers IT investments related to these categories. Other Strategic Initiative-related IT investments are covered in the Prefiled Direct Testimony of Joshua J. Jacobs, Exh. JJJ-1T (technology enablement efforts related to PSE's Clean Energy Implementation Plan ("CEIP")), the Prefiled Direct Testimony of Carol L. Wallace, Exh. CLW-1T (customer experience projects), and the Prefiled Direct Testimony of David J. Landers, Exh. DJL-1T (grid modernization projects).

II. PSE IS APPROPRIATELY INVESTING IN IT TO SUPPORT CLEAN ENERGY AND CUSTOMER NEEDS

A. Introduction to PSE's IT Strategy

Q. Please provide a high-level overview of PSE's IT strategy and vision.

A. PSE's mission is to be its customers' clean energy partner of choice. PSE is working toward that with its aspirational, climate-leadership goal of being a Beyond Net Zero Carbon energy company by 2045, while complying with

Washington's Clean Energy Transformation Act ("CETA")[1] aimed at carbon reduction. The core mission of PSE's IT strategy is to accelerate PSE's clean energy transformation through use of technology. In conjunction with that, PSE's IT strategy is to provide a seamless and secure integration of data and systems that will enrich the customer experience. To deliver on its IT strategy, PSE will focus on key technology areas that accelerate Company objectives and deliver innovative and sustainable solutions that are secure and reliable. The PSE IT strategy is based on the below objectives:

- Deliver business capabilities and enable customer, energy delivery, and equity targets through implementation of PSE's clean energy strategy "PSE 2030," and grid modernization technology projects.

- Enable a productive and collaborative workforce to support PSE's clean energy transformation through implementation of Digital Workplace tools, applications, and service improvements.

- Enable improved decision making through data analytics and predictive modeling to support improved operational effectiveness, customer experience, grid enhancements, and energy equity.

- Identify and leverage emerging technologies across IT to deliver business value and efficiency.

- Ensure the security of corporate data and assets through a robust Zero Trust Security model.

- Deliver scalable and flexible enterprise solutions though a cloud-first approach.

- Maintain key and critical systems to ensure a supported, modernized, and highly resilient technology platforms.

[1] Chapter 19.405 RCW.

PSE's IT strategy aims to build resilient, secure, and cost-effective technology solutions that are digitally integrated to improve grid and gas safety and reliability, enable clean energy solutions, and to also keep pace with evolving customer expectations. This vision is supported by a comprehensive investment plan consisting of the three major work streams noted above: Business Enablement, System Modernization, and Strategic Initiatives. I describe these in more detail below.

B. Risks and Challenges Associated with PSE's IT Strategy

Q. Are there any risks or challenges associated with PSE'S IT strategy?

A. Yes. Digital modernization has accelerated in the utility sector, and while the benefits are clear—including grid modernization, automation, improved customer interactions, and improved insights into customer needs—utilities must also plan for the risks and challenges that come with digitization, specifically those that pertain to cybersecurity, cloud-based services, and emerging technologies including artificial intelligence.

Q. What are the risks and challenges that cybersecurity poses to digital modernization?

A. Cybersecurity risks continue to require increased focus as the number of threats and bad actors targeting critical energy infrastructure is increasing. Data theft, billing fraud, and ransomware are as relevant to the utility industry as they are to other industries. Additionally, utilities must anticipate and protect against the risk

of large-scale disruption of transmission systems, substations, and generation sites caused by cybersecurity vulnerabilities and attacks. The rate at which cyber criminals specifically target operational technologies, which include the computers, data networks, and operator interfaces associated with electrical grid networks (often referred to as Supervisory Control and Data Acquisition or "SCADA" networks), continues to increase and tactics are becoming more complex and challenging to protect against.

The National Association of Regulatory Utility Commissioners ("NARUC") published guidance for evaluating utility proposals for cyber investments and outlined two approaches: compliance-based and risk-based protection. A compliance-based approach to securing the grid (e.g., North American Electric Reliability Corporation Critical Infrastructure Protection ("NERC-CIP")) by itself, is not sufficient. With the cyber landscape continually evolving, it is critical that utilities shift to a more comprehensive, risk-based approach that leverages a framework such as the National Institute of Standards and Technology ("NIST") 18-207 Framework recommended for critical infrastructure per Executive Order 13636. NIST's guidance states that a defense-in-depth (or multi-layered) approach is required to adequately protect operational technologies. This means that PSE and other utilities must go beyond compliance obligations to properly protect the electric grid and gas infrastructure to provide safe and reliable service to customers.

Q. How does PSE protect its infrastructure and service to customers from cyberattacks?

A. PSE leverages both compliance-based and risk-based protections to secure electric and gas infrastructure, and the costs to keep pace with protecting, monitoring, and responding to cyber threats in the rapidly changing threat landscape are increasing substantially. Compliance obligations such as NERC-CIP and Transportation Security Administration ("TSA") regulations continue to evolve and require increasingly comprehensive cyber protections and mitigating actions of which PSE is required to comply. PSE is committed to investing in the resources, skills, and systems necessary to provide an appropriate cybersecurity posture, but the cost required to support these efforts is escalating as bad actors quickly adapt their tactics to breach new technologies and challenge existing security protections. Known security costs are built into PSE's business plan; however, the volatility of the cyber threat landscape and new regulations required by various federal entities makes it difficult to anticipate and capture all costs required to properly protect PSE's systems from cyberattacks.

Q. Does PSE have a plan to mitigate the risk posed by cybersecurity?

A. Yes, PSE is tackling the cybersecurity risk through a variety of strategies. PSE's cybersecurity programs are based on the same national standards and frameworks used by leading companies in the energy and defense sectors. PSE participates in industry related cybersecurity programs that share best practices and actively work to improve the overall security posture for the industry. For example, PSE

holds an executive seat on the Energy-Information Sharing and Analysis Center ("E-ISAC") and is a member of the Downstream Natural Gas-Information Sharing and Analysis Center ("DNG-ISAC"). The E-ISAC and DNG-ISAC are the trusted sources for analysis and rapid sharing of cybersecurity information and threats for North America. PSE is also a member of the Electric Subsector Coordinating Council's ("ESCC") Cyber Mutual Assistance ("CMA") program, where PSE's Chief Information Security Officer served as chairperson from February 2019-August 2021. The CMA program is an industry framework developed at the direction of the ESCC to provide emergency cyber assistance within the electric power and natural gas industries. PSE is also part of a select group of utilities that participate in the national Cybersecurity Risk Information Sharing Program, which provides PSE with access to real time dashboards and intelligence based on data analyzed from other participating utilities.

In addition, PSE employs some of the most comprehensive security tools available to keep its infrastructure and information safe. PSE frequently evaluates its cybersecurity posture so additional investments are properly identified and funded. In addition to keeping its security tools current, PSE has strong policies and programs in place that assist in achieving its overall security goals, including vulnerability management, threat management, and compliance and awareness. PSE's cybersecurity team is also engaged in the evaluation of all new technologies (prior to purchase) and directly involved in technology projects so cyber controls are designed and built into each technology solution. Hardware and software providers must complete a comprehensive security addendum as part of

their contract to provide PSE with assurances of adequate cyber controls. Finally, to address the complexities and dependencies evolving between physical and cyber assets, PSE aligned its Physical Security team to the Security, Risk, and Compliance organization in 2021. This has streamlined mitigation efforts, particularly in PSE's generation, transmission, and distribution operations, where physical and cyber threats most often converge.

Q. What are the risks and challenges that cloud based services pose to PSE's IT strategy?

A. Cloud computing and Software as a Service ("SaaS") have become necessary in providing technology solutions to meet business challenges primarily because many technology vendors are driving customers to host technology solutions in the cloud by eliminating the option to host in their own data centers, or by investing and innovating only in their cloud-based offerings. Additionally, cloud computing and SaaS solutions can provide more affordable, secure, feature-rich, innovative, timely and reliable service in comparison to traditional on-premises solutions, which benefits customers.

However, while cloud offerings are typically cost neutral or cheaper than traditional on-premises solutions, most cloud costs that are unrelated to implementation cannot be capitalized, which causes a significant increase to annual operating expense. Progress has been slow to improve the regulatory treatment for cloud computing arrangements across the utility sector, and with this shift to operating expense, PSE is currently unable to earn a return on some

portion of cloud-based investments that are critical to running the business and for all intents and purposes, provide a similar service as traditional on-premises solutions. While PSE continues to make investments that provide the best service to customers irrespective of earning, the discrepancy in recovery further strains PSE financially. As PSE continues on executing the IT strategy, cloud costs will increase.

Q. Does PSE have any suggestions to mitigate the cost of migrating to cloud-based services?

A. One solution PSE supports is for the Commission to authorize, where appropriate, the ability for utilities to capitalize the full life-cycle cost of cloud-based services and earn a return on such investments, similar to what is allowed for on-premises technologies operated in PSE data centers. In 2016, NARUC adopted a resolution encouraging regulators to consider allowing utilities to do so. In the resolution, NARUC observed that the "business of electric, gas and water utilities is changing rapidly" and that other highly regulated industries, including financial services, healthcare, and telecommunications, and even government agencies, were transitioning to cloud-based services for a variety of beneficial reasons, including enhanced security, reliability, and flexibility. NARUC noted the inconsistency in permitting the classification of hardware and on-premises software as capital expenses, but not providing similar regulatory treatment to cloud-based technology when they perform similar functions. To encourage utilities to "make software investments based on which option best meets both the

needs of the utility and its customers" and not based on regulatory treatment, NARUC encouraged state regulators to consider providing similar regulatory treatment to both on-premises and cloud-based computing solutions.[2] Notably, some public utility commissions have already begun allowing this type of recovery, as provided in a recent order from the Idaho Public Utilities Commission.[3]

Q. Does PSE have a specific proposal at this time?

A. No. In the absence of clear policy direction from the Commission, PSE is not making a specific proposal in this case. However, PSE agrees with NARUC that utility service is evolving from an investment-based, to a more service-based model, and regulatory treatment should evolve accordingly. Some regulators have authorized earning on non-traditional investments, including earning on operating expenses as part of performance-based ratemaking. In 2019, the Washington legislature permitted earning on power purchase agreements under CETA. Before PSE presents a specific proposal for the regulatory treatment of cloud-based services, it would be helpful for the Commission to provide policy direction on this issue, specifically, whether the Commission supports the NARUC policy that allows similar regulatory treatment for both on-premises and cloud-based

[2] National Association of Regulatory Utility Commissioners, Resolution Encouraging State Utility Commissions to Consider Improving the Regulatory Treatment of Cloud Computing Arrangements (Nov. 16, 2016), http://pubs.naruc.org/pub/2E54C6FF-FEE9-5368-21AB-638C00554476

[3] *In the Matter of Idaho Power Company's Application for Costs Associated with Cloud Computing Arrangements*, Case No. IPC-E-20-11, Order No. 34707 (July 8, 2020).

computing solutions within reasonable guardrails, giving priority to investments that support system reliability and the protection of critical infrastructure from cyber threats. As PSE continues to execute on the IT strategy, the anticipated cost will increase.

Q. What are the risks and challenges that emerging technologies pose to PSE's IT strategy?

A. Emerging technologies can pose significant risks to organizations. Here are some of the risks associated with emerging technologies:

- Gaps in coverage resulting from changing products and services.
- Cybersecurity risks due to transformative technologies that enable new attacks.
- Implementing and supporting the new technology while still operating the old technology and the old processes and business model.
- Third-party risk that arises when relying on external providers for these new technologies—a reliance which is set to increase and create an even more complex ecosystem.
- Additional or different resource skillsets needed to implement and support emerging technologies including Cloud and SaaS.

Q. Does PSE have a plan to mitigate the risks posed by emerging technologies?

A. Yes. PSE IT is looking at emerging technologies that will meet business needs that will include guidance on use, skillsets needed, standards, and governance. PSE IT is engaging technology and utility industry experts to define best practices in relation to emerging technologies that can help PSE mitigate the risk. PSE has

already updated the Information Security and Acceptable Use policy to reflect the emerging risks of artificial intelligence including generative artificial intelligence.

C. Equity

Q. How does PSE IT ensure equity is a component of its Capital Portfolio process?

A. In 2023, PSE delivered and began using an Enterprise Project Portfolio Management tool to capture capital investment requests to be put forward for funding consideration as part of the five-year planning process. Energy equity was included in the solution design via a mandatory question that solicited the expected impact on Named Communities and/or Customer Benefit Indicators (CBIs). This approach resulted in the incorporation of energy equity considerations within the Corporate Spending Authorization ("CSA") tool for 2023/2028 CSAs as part of PSE's capital governance process.

` For more information on the Company's approach to equity, please refer to the Prefiled Direct Testimony of Troy A. Hutson, Exh. TAH-1T.

D. IT Investment Overview

Q. Please describe the types of programs or projects covered in your testimony.

A. As mentioned above, my testimony describes Business Enablement, System Modernization, and IT-related Strategic Initiatives.

Q. Please describe what a Business Enablement program or project is.

A. This category includes programs and projects that are identified by PSE business areas to support corporate strategies, customer needs, and other emerging business and compliance requirements. Business Enablement efforts include costs associated with acquisition, development, and installation of new systems, or the implementation of new business capabilities in existing systems. An example of a Business Enablement project is the Energy Management System Replacement.

Q. Please describe what a Systems Modernization program or project is.

A. This category represents capital efforts required to upgrade and maintain key and critical IT application and infrastructure platforms, and to ensure ongoing availability, stability, security, technical currency, and vendor support. By keeping applications and infrastructure equipment at supported levels, PSE can continue to receive critical system and security patches, take advantage of the latest technology features, and maintain license compliance as defined by support agreements. Programs or projects under this category directly support the corporate goal of 99.99 percent availability for systems that support critical business processes. Although some larger projects may be funded separately, most Systems Modernization work is funded annually under the IT Operational Program. The IT Operational Program is described in more detail later in my testimony.

Q. Please describe what a Strategic Initiative program or project is.

A. Work planned in this category delivers technology solutions that support PSE's strategic efforts including CETA compliance, clean energy investments, and improvements to the customer experience. These strategic efforts are sponsored and driven primarily by the business. Examples of a Strategic Project are IT investments that support PSE 2030.

Q. Please provide an overview of all Business Enablement, Systems Modernization and IT-related Strategic Initiative spending for which PSE seeks recovery in this case.

A. PSE seeks forward-looking recovery for approximately $373 million in technology investments expected to be placed in service during the calendar years 2025 and 2026. Exh. BEF-3 will provide detailed information supporting the above requests. Major projects costing more than $15 million are discussed below.

Q. Are there any external factors that may impact PSE IT's ability to deliver in accordance with the investment plan associated with the recovery request above?

A. Yes. There are many external factors that could influence delivery of the IT investment plan aligned with this rate case request, most of which are beyond PSE's control. Some external factors that impact PSE's IT investment plans are:

- **Inflation and rising technology and labor costs.** Price increases by strategic vendors have been common in recent years. The impact of any price increases will need to be assessed against planned projects to understand the impact to the overall investment plan. Inflation also factors into the rising cost of materials and labor that are used to deliver projects.

- **Vendor product availability.** PSE IT may be required to support new or emerging technologies to support PSE clean energy initiatives. As these are new or niche technical requirements, vendors may not be ready to release or have the capabilities in their products, which can cause delays.

- **New or emerging customer or business needs.** New technology projects may be required to support new or emerging customer or strategic business needs. Entry of new efforts into the plan may require portfolio rebalancing or the addition of unplanned funding.

Q. What impact could these external factors have on the proposed investment plan?

A. Over the course of a multiyear rate plan there will be times when the IT investment plan changes due to external factors, including the factors described above. This is the nature of running a complex business in a transformational time. The primary impacts expected will be related to changes in projected in-service dates and budgets. Impact will vary based on specific project needs, and the overall impact to annual investment plans. If investment plan changes do occur, IT will work within Corporate Finance's capital governance processes to identify solutions, which may include the addition of new capital budget, or the reallocation of capital across the remainder of the plan to achieve portfolio balancing. This may also result in the deferral of planned projects into future years to remain balanced with the original investment plan total expenditures

while still addressing non-controllable impacts. However, I emphasize that no change in conditions would cause PSE to compromise planned or implemented system enhancements that are designed or required to protect critical energy infrastructure or customer and/or system data. Critical energy infrastructure and data security protections are and will remain paramount priorities to PSE. These changes will also be reflective in the annul retrospective PSE provides. Please see the Prefiled Direct Testimony of Joshua A. Kensok, Exh. JAK-1CT, for additional information regarding Corporate Finance capital governance processes.

Q. Can you provide an example of how PSE has adjusted to external factors?

A. Two examples of PSE adjusting its investment plan following external impacts are PSE's implementation of the Advanced Distribution Management System ("ADMS") and WECC CIP-14 Audit Remediation during the last rate plan. In that case, the ADMS project was scheduled to complete in 2023 but vendor and product issues delayed final implementation, extending the program into 2024. Similarly, the WECC CIP-14 Audit Remediation project experienced significant fencing supply chain delays for one of the in-scope substations, as well as inflation of labor to complete the installation. As a result, additional funding was needed to complete installation work. Similar challenges are expected for the remaining three in-scope substations to be placed into service through 2025.

Q. How are IT investments identified and approved for funding within the IT Capital Portfolio?

A. For all Business Enablement, Strategic Initiatives, and some large Systems Modernization projects, a business case, known as a CSA document, is developed to support the need for each technology initiative. The CSA outlines the business problem or need, evaluates various solutions, and assesses the risk, cost, and benefits associated with each option. Total cost of ownership is considered at all decision points, with an emphasis on cost effectiveness and optimization of prior technology investments. All CSAs are reviewed and approved by business sponsors before they are submitted through PSE's Finance Department Corporate Capital Governance Process, where CSAs are evaluated for consideration and prioritized for investment in the five-year plan. The CSAs are prioritized in the Enterprise Portfolio Project Management ("EPPM") tool using a score based on criteria. This criterion includes, but is not limited to, Compliance, Safety, Operational, Reputational, Finance and Equity. Please see Kensok, Exh. JAK-1CT, for additional information on how the EPPM tool is used in for the Capital Portfolio. Additionally, any CSAs for technology programs or projects are reviewed and approved by PSE's Chief Information Officer ("CIO"). Decisions made under the Capital Governance process inform the final IT Capital Portfolio budget for subsequent years.

Smaller work efforts under the Systems Modernization category are funded annually, under the IT Operational Program. Proposals are solicited from each IT

department, and reviewed by the IT leadership team, who make annual funding decisions based on the business value and technology risk of each proposal. An annual CSA for the IT Operational Program in total is created and follows the same CSA approval process described above, including receiving review and approval from PSE's CIO.

Q. Once a program or project is approved within the portfolio, how is the technology solution determined?

A. PSE makes every effort to minimize cost by leveraging existing technology assets and maximizing their use. If an existing IT asset meets the majority of business and/or technical requirements, PSE will build upon the existing platform to the extent possible. By leveraging existing assets and vendor relationships, costs are optimized through volume discounts and lower integration costs, and implementation costs are kept in line through the use of in-house skill sets familiar with the technology to deliver solutions more quickly. When an existing system does not meet business requirements, multiple options are evaluated with a preference toward cloud or "purchased" products to keep development and maintenance costs lower, align with industry best practices, increase speed of implementation, and avoid development of highly customized systems that are difficult and costly to maintain.

Q. How do you design system implementation to minimize cost and risk?

A. Once selected, each system is designed to meet the stated business requirements, leverage out-of-the box capabilities to minimize customizations and to avoid over-reaching or gold plating with extraneous functionality. This helps to keep support and maintenance costs down and lowers the cost of future upgrades. Cybersecurity, data privacy, high availability, and disaster recovery capabilities are paramount, and designed into all systems in accordance with standards and principles defined by PSE's IT Architecture Team. PSE's IT Security also reviews all proposed solutions to ensure compliance and security obligations, such as the NERC CIP standards, which are included in each design. Systems are also designed for reuse, adaptability, growth, ease of operation and speed, and data governance and data management best practices are similarly embedded into designs to protect and maintain the accuracy of customer, asset, and employee data. This rigor is applied across all technology platforms to achieve maximum value from prior investments and to minimize the overall growth of ongoing IT expenses.

Q. What is PSE's process for procuring new technology and how does PSE get the best value?

A. All purchases follow PSE's standard contracting and procurement processes to obtain the best value for PSE and its customers. PSE's Procurement Team utilizes a competitive bid process so needed technology is competitively priced, is relevant to the utility industry and best serves customers. The competitive bid

process allows PSE to enable scale economies in pricing and ongoing maintenance, thereby providing a lower total cost of ownership on behalf of PSE's customers.

All technology purchases require the oversight of an IT Manager. The manager participates in the evaluation and analysis of the criteria used during the bid process, the selection of the technology, and final approval. The formal spend authorization process is automated through PSE's procurement system and uses built-in requirements to escalate to the IT Director or CIO level for additional approval when total spend exceeds pre-defined corporate limits. Additionally, in partnership with PSE Procurement, the IT Department engages with industry leading third party price and contract negotiation services. These partners provide PSE with updated information on market pricing and can guide PSE Procurement analysts related to negotiation strategies and leverage points PSE can utilize to obtain best price.

Q How are programs and projects governed to make sure they deliver within approved scope, schedule, and budget?

A. Project or program size generally dictates how governance is structured. At a minimum, an IT Manager is aligned with each project as the project sponsor and is responsible for managing the scope, schedule, and budget for the project. Business Enablement efforts will also have a business sponsor assigned. Programs and medium to large projects will have Project Managers assigned, and governance will include sponsor meetings and a formal steering committee. Some

very large programs and projects will also have an Executive Sponsor assigned and will convene an Executive Steering Committee. Regardless of the size, the governance structure is responsible for program or project oversight, key decision making, risk mitigations, and approval of any changes to scope, budget, or schedule.

PSE IT has also deployed a scalable portfolio management oversight for all IT capital efforts. PSE has created playbooks for the four types of projects:

- **Technology Refresh:** Refresh for technology to ensure supportability and reliability.
- **Small Projects:** Projects with low complexity and few risk factors.
- **Medium Projects:** Projects that involve moderate complexity and risk factors.
- **Large Projects:** Projects with a high level of risk or impact, justifying a higher level of governance and oversight.

Depending on the size of the project, the playbooks guide the project managers through the required processes and deliverables. Additionally, each playbook defines the project governance checkpoints and required approvals. All programs and projects submit a monthly budget forecast which enables regular review of expected spend. Any program or project requiring a scope, schedule, or budget update is required to complete a formal change request that, after approval by the Steering Committee and project change orders, are captured and documented on the project risk, issues, and decision logs for detailed tracking.

Q. Are there any IT programs or projects with an expected spend of at least $15 million over the course of the multiyear rate plan for which PSE is seeking recovery in this case?

A. Yes. There are several programs and projects that meet this criteria, including:

- IT Operational Program
- Cyber and Physical Security Program
- SAP S/4 HANA Migration project

Details on each are outlined below.

III. IT INVESTMENTS EXPECTED TO BE PLACED INTO SERVICE FROM JANUARY 1, 2025 THROUGH DECEMBER 31, 2026

A. Overview of IT Investment to Be Placed Into Service During the Period of January 1, 2025 Through December 31, 2026.

Q. Please provide an overview of all IT spending for which PSE seeks recovery related to the period of January 1, 2025 through December 31, 2026.

A. PSE seeks recovery of approximately $365.6 million in recovery for IT investments placed into service during this period. This includes $120.1 million of spend related to Business Enablement efforts, $198.2 million in Systems Modernization investments and $47.3 million in IT Strategic investments. A detailed list of all IT spending during this period for which PSE seeks recovery is provided in Exh. BEF-3, while details supporting major programs and projects related to this request are discussed below.

B. Major Programs and Projects Placed Into Service During the Period of January 1, 2025 Through December 31, 2026

1. IT Operational program.

Q. Please describe the IT Operational program.

A. PSE's IT Operational program is an ongoing program that ensures key and critical infrastructure and applications supported by IT are kept technically current and maintained under vendor support. Work under the IT Operational program is funded annually, with proposals submitted from across IT. The IT leadership team reviews and makes funding decisions based on business value and risk of each proposal. By keeping PSE's IT systems at supported versions, this ensures that systems will continue to receive critical patches from vendors, be able to take advantage of the latest features, and keeps IT assets at acceptable license levels as defined by vendor support agreements. This helps enable IT to deliver more reliable service to the business and PSE's customers. Work under this program primarily supports the following areas of IT:

- **IT Applications**. Operational work to ensure the approximately 400 applications in production are kept technically current and are properly maintained in compliance with our vendor support agreements. This program provides funding for critical applications such as the Energy Management System, Gas Control System, Outage Management System, SAP systems (Finance, Human Resources, Call Center, Billing, and Asset Management), Metering, PSE.com, and other critical business systems.

- **IT Infrastructure.** Consists of the computing and telecommunications hardware and software upon which critical business systems and capabilities are built. This is largely the IT equipment housed in PSE data centers, including 362 physical servers hosting over 4,424 virtual servers, virtual desktops, storage hardware, and the network equipment and connectivity

infrastructure (fiber, radio, and microwave) that enable telecommunications throughout PSE's service territory.

Q. Has work on the IT Operational program started?

A. Yes. As described in testimony above, the IT Operational program is an ongoing operational program, with specific work identified and prioritized by IT leadership for funding in the following year. All work is typically placed in service in the year for which it is funded.

Q. Is PSE seeking to recover costs related to the IT Operational program in this proceeding?

A. Yes. The total amount requested is approximately $78 million, which includes $41 million requested for 2025 and $37 million for 2026. Additional details on the IT Operational program spend during this period can be found in Exh. BEF-3.

Q. Because work on the IT Operational program has already started, please describe components of the program, including timeline for delivery.

A. As mentioned above, work under the IT Operational program is funded annually and proposals are submitted from across IT. IT leadership team reviews these to prioritize work for funding in the next year. The IT Operational program is broken into a separate CSA and funded to support the following types of projects:

- **IT Operational – Telecom.** IT Infrastructure's Telecom teams are responsible for maintaining PSE's vast telecommunications infrastructure comprised of telephones, radio and microwaves, fiber optic cable, towers, and SCADA systems which enable telecommunications. IT Infrastructure's operational work will ensure key and critical Telecom

applications and systems supported by IT are kept technically current and maintained under vendor support. Work under the IT Operations – Telecom category is funded annually, with proposals submitted by IT Telecom teams. Please see Exh. BEF-4 for additional information.

- **IT Operational – Capitalized Support and Maintenance Agreements.** This represents the allowable conversion of operating expense to capital as it relates to PSE's software licensing, maintenance, and support agreements with vendors. IT works with PSE's Property Accounting group to leverage Federal Energy Regulatory Commission guidelines for asset capitalization and to ensure the right documentation and term agreement is in place to support any capitalization. Please see Exh. BEF-4 for additional information.

- **IT Operational – Capitalized Cloud Services Agreements.** This represents the funding for allowed capitalization of SaaS applications and cloud platforms. This includes enterprise-wide costs absorbed by IT such as costs associated with the ServiceNow platform, Microsoft 365 platform which provides corporate email to all PSE employees and contractors, and other applications that are used across PSE. Please see Exh. BEF-4 for additional information.

- **IT Operational – Technology Reliability: Software.** These projects fund the non-discretionary capital efforts required to upgrade and maintain key and critical IT application platforms such as the Energy Management System, Gas Control System, Outage Management System, SAP systems (Finance, Human, Resources, Call Center, Billing, and Asset Management), Metering, PSE.com, among many other critical business systems and to ensure ongoing availability, stability, security, technical currency, and vendor support. Please see Exh. BEF-4 for additional information.

- **IT Operational – Technology Reliability: Hardware.** These projects fund the non-discretionary efforts required to upgrade and maintain key and critical infrastructure platforms and assets, and to ensure ongoing availability, stability, security, technical currency, and vendor support. The infrastructure covered under this category consists of the computing hardware upon which critical business systems and capabilities are built. This includes the IT equipment housed in data centers (~2,700 servers, batteries, etc.), end user devices, such as laptops, all corporate network related systems and hardware and other required hardware upgrades, enhancements, and end-of-life replacements. Please see Exh. BEF-4 for additional information.

- **IT Operational – Running the Business of IT.** These projects fund the non-discretionary efforts to support the running of IT. An example of work funded under this effort are mandatory yearly upgrades to Service Now. Please see Exh. BEF-4 for additional information.

Q. What are the expected benefits of the IT Operational program?

A. Efforts funded under the IT Operational program are required to maximize the value and asset life of PSE's technology investments. Completion of the IT Operational program work keeps PSE's IT systems secure, stable, and reliable, and ensures that PSE IT will continue to receive critical patches from vendors, be able to take advantage of the latest features, and keeps IT assets at acceptable license levels as defined by vendor support agreements.

Q. How is the program team keeping PSE management informed during the course of the program?

A. Larger efforts under the IT Operational program are run as formal projects, have a primary IT Sponsor assigned, and follow the IT Project governance structure requirements, as described above. Monthly status reports and budget forecasts are submitted, and any projects reporting risks, issues or potential changes to project budget or schedule are discussed in monthly IT Portfolio meetings. Smaller efforts are assigned to a primary IT Sponsor, who is responsible for managing the work to completion, completing monthly budget forecasting

Q. Have there been, or are you expecting, any material changes affecting program scope, schedule or budget?

A. No. The IT Operational program is planned and funded as an annual effort, with all associated work placed into service during the year in which it was funded. The CIO is responsible for completing annual program plans, identifying work for future years, and working with the IT leadership team when any changes are required to specific efforts during a calendar year. This may include deferring efforts in progress to help offset additional budget required for a more critical effort or allowing new projects to start if additional funding becomes available as efforts complete under projected spend. All potential program changes to the Portfolio are discussed at monthly, with any changes approved enacted upon and logged as a portfolio decision. For additional detail on this program see Exh. BEF-4.

2. <u>Cyber and Physical Security program.</u>

Q. Please describe PSE's Cyber and Physical Security program.

A. Similar to the IT Operational program, PSE's Cyber and Physical Security program is an ongoing program of work that secures annual funding to support both cyber and physical security project needs. PSE's Chief Information Security Officer and Director of Security, Risk & Compliance, serves as the primary sponsor for this program. This department is responsible for developing the roadmaps that support this work and include the following areas:

- **Cybersecurity.** Cybersecurity protects cyber assets, such as computers and data, from unauthorized access. PSE's cybersecurity program is based on the NIST CSF v1.1. Utilizing this framework provides PSE with an accepted reference point for the review of PSE's ability to protect its assets against cybersecurity threats. These standards are followed by leading companies in the energy and defense industries, and PSE has standardized assessments biennially against those standards, conducted by external security firms. The primary objectives for projects under this investment category are to improve PSE's cybersecurity posture, better prepare and protect PSE against future cyber threats, and maintain compliance with federal requirements. Without this focus, PSE would not have been able to successfully protect against the millions of vulnerabilities that have been introduced to the IT landscape over the last several years.

- **Physical Security.** Physical Security describes security measures that are designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm. As such, the primary objective of work funded under this category is to protect PSE's physical assets and personnel. The use of technology in protecting physical security assets is expanding. Traditional physical security functions and countermeasures, such as alarm monitoring, security cameras, and even facility access, now depend on integrated technology platforms. To address the complexities and dependencies associated with the convergence of physical and cybersecurity, PSE aligned the Physical Security team to the Security, Risk and Compliance organization in 2021. As a result, Physical Security investments are included in IT rate recovery requests.

Q. Has work on the Cyber and Physical Security program started?

A. Yes. As described above, the Cyber and Physical Security program is an ongoing program, with specific work identified by PSE's Security teams, and prioritized by PSE for funding in the following year. The majority of work is expected to be placed in service in the year for which it is funded.

Q. Is PSE seeking any cost recovery related to the Cyber and Physical Security program in this proceeding?

A. Yes. The total amount requested for the Cyber and Physical Security program across all years included in the rate case is approximately $32.3 million which includes $21 million requested for 2025, and $11.3 million for 2026. Please refer to Exh. BEF-3 for additional details on this spend.

Q. Because work on the Cyber and Physical Security program has already started, please describe components of the program, including timeline for delivery.

A. As mentioned above, work under the Cyber and Physical Security program is funded annually. Specific work is identified by PSE's Security teams for incorporation into their roadmaps and prioritized for funding. Best practices, current security state, third party assessment feedback, and PSE architectural direction are all considered when evaluating solutions and determining future-year projects to be undertaken/funded by the program. The Cyber and Physical Security program focuses on mitigating security vulnerabilities, preventing exposures, and managing IT compliance requirements for the Company's cyber assets. While many of the projects funded by this program are small and deployed within a few months (e.g., deploying vulnerability software to scan Operational Technology (OT) environments), some are large and will take several years to complete.

An example of a large project funded by this program is the implementation of technology and services to support a Zero Trust cybersecurity model across the Enterprise. Zero Trust is a cybersecurity model where information systems and services are designed to enforce accurate, least privilege, and dynamic access decisions to assets and users. While this project kicked off in 2023, deliverables are complex and will be deployed through 2026. The Physical Security program focuses on modernizing physical security systems at non-NERC PSE facilities to ensure that they are highly available, scalable and resilient. Facilities are scoped in collaboration with Operations teams in the first quarter of each year and the schedule is based on risk level presented by existing security countermeasures and current threat landscape. Deliverables may include security cameras, video systems, intrusion detection systems, perimeter fencing and electronic key systems. All of these physical security measures combine to provide a layered defense strategy in the protection of PSE-owned assets and sites. Current deliverables planned through 2026 include:

- Deploying new security camera systems to high-risk sites.
- Upgrading existing intrusion detection systems with modern technology and installing new intrusion detection systems at high-risk sites.
- Enhancing security lighting systems and installing ground-based radar systems and thermal cameras at high-risk sites.
- Replacing existing chain-link fencing with anti-cut/anti-climb fencing at high-risk sites.
- Replacing physical brass keys and improve physical access management capabilities and operational burden.

Q. What are the expected benefits of the Cyber and Physical Security program?

A. Protecting PSE's personnel and investments in infrastructure, facilities, and technology is the primary driver for the Cyber and Physical Security program. PSE must secure these assets against current and future threats. The need to be able to withstand and recover rapidly from deliberate attacks against PSE assets is a necessity for the continued service reliability PSE's customers require.

Additional benefits include:

- **Ability to proactively respond to the ever-changing multitude of risks.** Technology continues to be foundational for all areas of critical business operations, and security threats continue to increase in both number and sophistication, warranting a proactive approach to mitigate this risk.

- **Reduction of risk to PSE facilities and personnel.** As mentioned above, technology and traditional physical security measures are converging, introducing new and complex threats that must be addressed.

- **Reduction of financial risk.** The cost to respond to a security breach can have significant impact on a company's financials. Preventative focus and investment allows PSE to help mitigate the risk of these costs being passed on to customers.

- **Reduction of customer risk.** Investments and efforts undertaken help protect customer's confidential and sensitive data; and

- **Assured regulatory compliance**. New regulations are expected for existing and future energy assets. PSE must maintain security requirements to best protect customers and availability of service.

Q. How is the program team keeping PSE management informed during the program?

A. All efforts under the Cyber and Physical Security Program are run as formal projects and follow the IT Project Governance structure requirements, as described above.

Q. Have there been, or is PSE expecting, any material changes affecting program scope, schedule, or budget?

A. Yes. There are a few areas where there have been material changes or PSE expects to see material changes. The Physical Security WECC CIP-014 Mitigation Program was initially expected to be completed in 2025 with an overall budget of about $17.9 million. PSE adjusted the overall budget to approximately $30 million. The primary drivers for the budget increase are supply chain issues delaying receipt of material, and the increased cost of materials and labor due to inflation. For additional detail on this program see Exh. BEF-5.

3. <u>Energy Management System Platform Replacement project.</u>

Q. Please describe PSE's Energy Management System ("EMS") Platform Replacement project.

A. The EMS Platform Replacement project is to replace PSE's legacy General Electric platform with a modern, advanced EMS. This will improve PSE's operational capabilities and ease of maintenance by simplifying the underlying architecture and introducing new functionality, such as:

- Streamlined product and patch releases with vendor managed source code.
- Simplified modern architecture that will rapidly evolve to address PSE requirements and NERC growth.
- Enhanced user interface.
- Improved system administration.
- Operator training simulator to better represent real-time scenarios.
- Simplified database management and improved release efficiency.

Q. Why is PSE investing in the EMS Platform Replacement project?

A. PSE's NERC regulated systems, which support and control PSE's electric transmission and power generation facilities, are entering into an obsolete state. Running end-of-life systems introduces the risk of irrevocable damage and costly downtime in the event of failure. These costs can include fines up to $1,000,000 a day based on the severity and duration of an incident. Operation and control of the transmission system has become more complex over the last decade due to fast evolving technology of transmission and generation assets, stringent NERC regulations, and a resultant increase in real-time operational workload. Within PSE's Transmission Control Center (Load Office), the need for control room operators to have more effective and reliable tools to operate the grid and maintain high situational awareness has emerged. The EMS is the most critical and the primary software application used in the transmission control center. The EMS used by PSE will lose vendor support, and will no longer receive critical

security updates in 2026, so the planning effort started in 2022 with some components going into service in 2025, before final project completion in 2026.

Q. Has work on the EMS Platform Replacement project started?

A. Yes. The project team completed the planning phase of the EMS Platform Replacement project. PSE has engaged work with Power Systems Consulting to support the requirements documentation, gap analysis, and the end-to-end RFP process which will focus on establishing the supplier performance and risk management governance processes and tools. The EMS Platform Replacement team published the RFP to four vendors. After reviewing responses and onsite demonstrations, the EMS Platform Replacement team has received approval from the sponsors of the recommended industry leader software vendor.

Q. Is PSE seeking any cost recovery related to the EMS Platform Replacement project in this proceeding?

A. Yes. The estimated cost for the EMS Platform Replacement project is approximately $30.3 million over four years. The project will be placed in-service in 2026.

Q. Because work on the EMS Platform Replacement project has already started, please describe components of the project, including timeline for delivery.

A. Planning and project initiation for the EMS Platform Replacement project began in 2023. A majority of 2024 will be working with PSE's selected vendor on the design of the new EMS platform. The execution phase is planned to start in 2024 with the project going into service in 2026.

Q. What are the expected benefits of the EMS Platform Replacement project?

A. Adopting up to date EMS technology will improve PSE's situational awareness capabilities, operational efficiency, and ability to maintain the EMS system. Increased frequency of software upgrades will guard against obsolescence and will better address the evolving nature of the industry. Benefits include:

- Improved electrical grid reliability and resiliency.
- Improved operational efficiency.
- Improved situational awareness capabilities.
- Improved vendor engagement.
- Increased frequency of software upgrades
- Reduced EMS operational complexity.
- Reduced future maintenance and upgrade costs.

Q. How is the program team keeping PSE management informed during the roll out of the EMS Platform Replacement project?

A. The governance structure used for the program aligns with standard PSE IT governance structure requirements for technology programs and projects described above. Primary IT and business sponsors are assigned to the project and a Steering Committee comprised of leaders from across PSE and IT meet regularly to monitor the project. Additionally, monthly project status reports are created and reviewed in Steering Committee meetings.

Q. Have there been any material changes affecting program scope, schedule, or budget?

A. Yes. Due to the complexity of implementing the EMS system, the project began one year earlier in 2022 and will be placed into service in 2026.

For additional detail on this project see Exh. BEF-6.

4. <u>SAP S/4 HANA Migration project.</u>

Q. Please describe PSE's SAP S/4 HANA Migration project.

A. The SAP S/4 HANA Migration project is a large Systems Modernization effort to upgrade all SAP system components due to system obsolescence. SAP is an Enterprise Resource Planning ("ERP") software that PSE uses as a centralized system to access and share common data for core business functions, such as financial and accounting, human resources, customer relationship management,

inventory management, and many others. SAP is the most-used ERP software on the market and contains hundreds of fully integrated modules that cover nearly every aspect of business management. PSE's current SAP system utilizes version 6.0 of SAP ERP Central Component, referred to as "SAP ECC 6.0." SAP ECC 6.0 will be end-of-life and the SAP S/4 HANA Migration project will work to upgrade PSE's SAP system to SAP Business Suite 4 SAP HANA, which is commonly known as "SAP S/4 HANA" and is the latest ERP solution offered by SAP. As the technology landscape is changing, PSE will potentially look at alternative options available in the marketplace.

Q. Has work on the SAP S/4 HANA Migration project started?

A. No. Work is expected to begin in 2024 and complete in 2026. Specific components of PSE's SAP system will be upgraded and placed into service accordingly.

Q. Is PSE seeking any cost recovery related to the SAP S/4 HANA Migration project in this proceeding?

A. Yes. The estimated cost the SAP S/4 HANA Migration in the multiyear rate plan is approximately [redacted] million, with [redacted] million of expected spend to be placed in service during 2025 and [redacted] million in 2026. The estimated annual spend placed in service each year assumes that individual components of the overall SAP systems can be placed into service as they are upgraded, and will be solidified as the project team completes detailed planning.

Q. Given that the SAP S/4 HANA Migration project has not yet started, please describe how specific project work will be identified.

A. The PSE SAP team is currently working with other utilities who are in progress with their S/4 HANA migrations to understand how they are sequencing work to help with development of the overall project approach. Additionally, the team has engaged with PSE's SAP vendor partner for guidance on project approach and is utilizing PSE's industry leading strategic partner for development and support work, for a best practice perspective. Finally, the PSE SAP team is additionally working with key PSE business partners to understand their business processes and to determine areas of improvement or pain points that can be addressed during the S/4 HANA migration, as the new platform offers several areas of new functionality.

Q. Please describe currently planned system efforts.

A. PSE's SAP ECC 6.0 system will be replaced with the SAP S/4 HANA system. As part of this process, many currently installed SAP modules will require upgrades, including the SAP Financial and Accounting module. This model supports all financial processes across PSE and is critical to PSE operations. The upgrade will allow for additional functionality including streamlined financial processes, making possible real-time financial data analysis.

In addition, migration to SAP S/4 HANA would allow PSE to eventually migrate SAP to the cloud; PSE will review this possibility and decide at a future date. At

this time, PSE will run all SAP environments on hardware and equipment residing in PSE's data centers.

Q. What are the expected benefits of the SAP S/4 HANA Migration project?

A. Although the primary benefit is mitigation of risk related to running PSE's critical systems on obsolete and non-supported platforms, secondary benefits are widespread and associated with all upgraded modules. Key benefits include:

- **Ability to support strategic business needs.** SAP S/4 HANA is already in use globally and offers significant new functionality that PSE can use. Additionally, SAP is expected to continue investment into expanded functionality for SAP S/4 HANA in the future.

- **Improved customer experience.** Many customer services depend on SAP functionality and migrating to the latest platform for ongoing availability, stability, and resiliency of service. This migration will support services in the PSE Call Center.

- **Streamlined financial processes.** SAP S/4 HANA combines the disparate data structure associated with Financial Asset Accounting, Controlling, Profitability Analysis, and Material Ledger into a single data structure referred to as the Universal Journal. This eliminates many aggregate and index tables, resulting in increased ability to access data needed for critical business support and resulting in significantly increased process efficiency, including shorter month-end and year-end closing.

For additional detail on this project see Exh. BEF-7C.

IV. CONCLUSION

Q. Does that conclude your prefiled direct testimony?

A. Yes, it does.