EXH. MFH-1T
DOCKETS UE-22___/UG-22___
2022 PSE GENERAL RATE CASE
WITNESS: MARGARET F. HOPKINS

BEFORE THE
WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION, **Complainant,** **v.** **PUGET SOUND ENERGY,** **Respondent.**	**Docket UE-22____** **Docket UG-22____**

PREFILED DIRECT TESTIMONY (NONCONFIDENTIAL) OF

MARGARET F. HOPKINS

ON BEHALF OF PUGET SOUND ENERGY

JANUARY 31, 2022

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (NONCONFIDENTIAL) OF MARGARET F. HOPKINS

CONTENTS

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (NONCONFIDENTIAL) OF MARGARET F. HOPKINS

LIST OF EXHIBITS

PUGET SOUND ENERGY

PREFILED DIRECT TESTIMONY (NONCONFIDENTIAL) OF MARGARET F. HOPKINS

I. INTRODUCTION

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

A. My name is Margaret F. Hopkins, and my business address is Puget Sound Energy, Inc., P.O. Box 97034, Bellevue, Washington 98009-9734. I am employed by Puget Sound Energy ("PSE") as Senior Vice President of Shared Services and Chief Information Officer.

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

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

Q. What are your duties as Senior Vice President of Shared Services and Chief Information Officer for PSE?

A. In my role as Chief Information Officer, I am responsible for PSE's technology and cyber security strategy, and for delivering technology solutions that enable PSE's strategic plan. As Senior Vice President of Shared Services, I oversee PSE's Supply Chain, Corporate Shared Services and the Project Practices Center of Excellence.

Q. What topics are you covering in your testimony?

A. My testimony provides an overview of PSE's Information Technology ("IT") vision and strategy and highlights key risks and challenges IT faces in support of corporate strategic efforts to achieve beyond net zero carbon emission by 2045. I also address how IT supports corporate commitments to safety, clean energy, and reliability. The purpose of my testimony is to illustrate the critical role that IT plays in making sure PSE can meet its obligations to customers and the state of Washington. I also explain why the IT modernization programs PSE is pursuing are necessary so PSE can meet customer expectations to improve the reliability of PSE's infrastructure, to protect PSE from cyber threats, and to enhance the experience customers have with their energy usage.

Testimony related to IT capital investments already placed in service or expected to be placed in service during the multiyear rate period is provided in the Prefiled Direct Testimony of Suzanne L. Tamayo, Exh. SLT-1T.

Q. Are you making any specific request on behalf of PSE in your testimony?

A. No, not at this time.

II. PSE IS APPROPRIATELY INVESTING IN INFORMATION TECHNOLOGY TO SUPPORT CUSTOMER NEEDS NOW AND IN THE FUTURE

Q. Please provide a high-level overview of PSE's strategy for making technology investments.

A. Utilities continue to undergo tremendous change and transformation, and the pace of that change is increasing dramatically as the movement toward clean energy and decarbonization accelerates. This is especially true in Washington State as utilities comply with the Clean Energy Transformation Act ("CETA"), which creates additional technology needs to modernize grid infrastructure to improve reliability, strengthen cyber security protections, and improve the tools customers can use to engage with PSE for their energy needs and preferences. IT assets are now as foundational as the pipes and wires that deliver service to customers, and are inextricably linked to advancing, securing, and enabling the day-to-day operation of PSE's gas and electric service and clean energy strategy. PSE's customers benefit from these IT investments because the investments advance the resiliency and reliability of PSE's electric and gas infrastructure and make it easier for customers to interact with PSE to access the information they need about their utility services. As an example, the self-service capabilities launched with PSE's Get To Zero ("GTZ") program transformed the ability for customers to quickly obtain information regarding their energy consumption, outages, billing and payment options, low-income assistance, and various opportunities to

participate in energy efficiency and clean energy services. GTZ program specific benefits are detailed in Tamayo, Exh. SLT-6.

PSE's technology 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 strategic plan consisting of three major work streams: Strategic Initiatives, Business Enablement, and System Modernization.

Q. What type of work is Strategic Initiatives?

A. Work planned in this category delivers technology solutions that support PSE's strategic efforts including CETA compliance, grid modernization, and improvements to the customer experience. These strategic efforts are sponsored and driven primarily by the business. Examples include Customer Usage Disaggregation and Presentment (as detailed in the Prefiled Direct Testimony of Carol L. Wallace, Exh. CLW-1T), and Time Varying Rate Pilot (as detailed in the Prefiled Direct Testimony of William T. Einstein, Exh. WTE-1CT). Additional strategic technology investments required to support PSE's Clean Energy Implementation Plan are discussed in the Prefiled Direct Testimony of Joshua J. Jacobs, Exh. JJJ-1T.

Q. What type of work is Business Enablement?

A. Work planned in this category includes projects that are identified by PSE business areas to mitigate risk, adhere to compliance obligations, and support demands driven by customer needs and emerging business requirements. Examples include GTZ-Integrated Work Management, Advanced Distribution Management System, and PSE's Data Enablement and Enrichment Program. These and other Business Enablement projects are discussed in Tamayo, Exh. SLT-1T.

Q. What type of work is System Modernization?

A. This work stream represents capital efforts required to upgrade and properly maintain key and critical IT systems. These upgrades are vital to asset health and reliability and to protect against ongoing cyber threats and vulnerabilities. Keeping applications and infrastructure equipment at supported levels allows PSE to receive critical system and security patches, take advantage of the latest features, and maintain license compliance as defined by support contracts and agreements. It is important to note that these IT investments are perpetual, and do not drive any specific cost savings. They are required by the software and hardware vendors to receive support for break/fix issues, maintain compliance and contractual obligations, and close security vulnerabilities. Examples include Data Center Hardware Refresh, SAP S4 HANA Migration, and Cyber and Corporate Security Programs. These and other System Modernization initiatives are discussed in Tamayo, Exh. SLT-1T.

III. RISKS AND CHALLENGES ASSOCIATED WITH DIGITAL MODERNIZATION

Q. Are there any risks or challenges associated with digital modernization?

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

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

A. Cyber security risks require increased focus as the number of threats and bad actors targeting critical energy infrastructure continues to rise. Data theft, billing fraud, and ransomware are as relevant to the utility industry as they are to other industries. However, utilities must also anticipate and protect against the risk of large-scale disruption of transmission systems, substations, and generation sites due to network attacks and exploitation of vulnerabilities in the supply chain.

There is a clear uptick in the rate at which cyber criminals specifically target operational technologies ("OT"), which include the computers, data networks and operator interfaces associated with electrical grid networks (often referred to as "SCADA" networks). Because these OT networks are increasingly integrated with corporate IT systems for the purposes of automation and improved

operational performance, they have increased exposure, and are ultimately more vulnerable to cyber-attacks.

The National Association of Regulatory Utility Commissioners ("NARUC") recently published guidance for evaluating utility proposals for cyber investments. The guidance outlines two approaches: compliance-based and risk-based protection. A compliance-based approach to securing the grid (e.g., 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 OT. 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.

PSE leverages both compliance-based and risk-based protections to secure electric and gas infrastructure. However, the costs to keep pace with a quickly changing threat landscape and the resulting actions PSE must take to protect, monitor, and respond to cyber threats, are increasing at a rapid pace. Existing compliance obligations (e.g., NERC CIP) and newly developed compliance directives, such as those being driven by the Transportation Security Administration ("TSA") and the Cyber Security and Infrastructure Agency in

response to the recent Colonial Pipeline attack, will introduce increasingly comprehensive cyber protection requirements and mitigating actions. PSE is required to comply with these directives and anticipates investments to accelerate over the next five to ten years.

PSE is committed to investing in the resources, skills, and systems necessary to provide an appropriate cyber security posture. However, the cost required to support these efforts is escalating as compliance obligations expand and cyber threats grow and become more disruptive. Known security costs are built into PSE's business plan. However, due to the volatility of the cyber threat landscape and the potential for unplanned cyber expenditures and compliance obligations driven by federal entities such as TSA and NERC, it is difficult to anticipate and capture all costs that will be required to properly protect PSE's systems from cyber-attacks.

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

A. Yes, PSE is tackling the cyber security risk through a variety of strategies. PSE's cyber security 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 cyber security 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 cyber security 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 chairwoman for the past two years. 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 and is constantly evaluating 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 cyber security 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 has taken an additional and proactive step to merge its Physical and IT Security departments together, under the Chief Information Security Officer. This will help streamline mitigation efforts, particularly in PSE's generation, transmission and distribution operations, where most often the physical and cyber threats converge.

Q. What are the risks and challenges that cloud based services pose to digital modernization?

A. Cloud computing and Software as a Service ("SaaS") have become necessary in providing technology solutions to meet business challenges for two primary reasons:

1. Many technology vendors force companies to host technology solutions in the cloud by eliminating the option to host in their own data centers;

2. IT often looks to cloud computing and SaaS solutions to provide more affordable, secure, timely and reliable service, which in turn benefits customers.

While cloud offerings are typically cost neutral or cheaper than traditional on-premise solutions, most cloud costs that are unrelated to implementation cannot be capitalized, which causes a significant increase to annual operating expense. Little progress has been made 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 cloud-based investments that are critical to running the business and for all intents and purposes, provide a similar service as traditional, on-premise solutions.

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. In 2016, NARUC adopted a resolution encouraging regulators to consider allowing utilities to do so.[1] 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-premise 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.

[1] 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.

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-premise and cloud-based computing solutions.

Q. Are there any external factors that are impacting PSE IT's ability to deliver on its IT strategy?

A. Yes. Currently, COVID and the supply chain issues have had a significant impact on the availability of hardware components needed for PSE's data centers, networks, cyber security, and telecommunications. This is due to a world-wide shortage in chip production and wide scale shipping delays of hardware and firmware to technology manufacturers and providers. Several of PSE's strategic technology vendors, including Microsoft and Cisco, have signaled that significant price increases are expected for their products and services starting in 2022, citing

COVID and supply chain issues as the cause. These external factors directly affect PSE's ability to deliver projects on schedule and within budget. Supply chain constraints alone shifted the in-service dates of several IT projects from 2021 to 2022. Given the trajectory of COVID and the continued supply chain issues, we can expect similar impacts throughout the multiyear rate plan.

Further, the impending cyber security compliance directives from TSA (as noted earlier in my testimony) will introduce unplanned work and expenditures in 2022 and beyond. TSA has provided no insights into the depth and breadth of these future directives, except to state that they are coming. This limits PSE's ability to estimate the cost and timing to comply with the directives until they are imposed and evaluated.

PSE IT will continue to monitor these external and non-controllable risks and will work in concert with Corporate Finance to appropriately reallocate IT investments within reasonable guardrails, giving priority to investments that support system reliability and the protection of critical infrastructure from cyber threats.

IV. CONCLUSION

Q. Does that conclude your prefiled direct testimony?

A. Yes, it does.