BEFORE THE PUBLIC UTILITY COMMISSION

OF THE STATE OF OREGON

UE 319

Information Technology

PORTLAND GENERAL ELECTRIC COMPANY

Direct Testimony and Exhibits of

Cam Henderson
Behzad Hosseini
Travis Anderson

February 28, 2017

Table of Contents

I.   Introduction

1 **Q. Please state your names and positions with Portland General Electric (PGE).**

2 A.   My name is Cam Henderson. I am the Vice President of Information Technology (IT) and

3   Chief Information Officer (CIO) at PGE.

4   My name is Behzad Hosseini. I am a Director of the Office of CIO for PGE.

5   My name is Travis Anderson. I am the Information Security Director and Manager of

6   IT Risk Management at PGE.

7   Our qualifications appear in Section V of this testimony.

8 **Q. What is the purpose of your testimony?**

9 A.   We explain PGE's request for $94.4 million in IT costs in 2018 and compare it to 2016

10   actuals of $73.3 million.

11 **Q. How is your testimony organized?**

12 A.   After this section, we have four sections:

13   • Section II: 2020 Vision Program Update

14   • Section III: IT O&M Costs

15   • Section IV: Information Security Operation Center (ISOC)

16   • Section V: Summary and Qualifications

17 **Q. What activities or functions does PGE consider as IT?**

18 A.   IT consists of the departments responsible for developing, operating, and maintaining our

19   computer, cyber, information, and communication systems. These systems are becoming

20   increasingly important to all aspects of PGE's operations (with increasing scope, reliance,

21   and use). In addition, the threats to these systems are becoming more numerous and varied.

22   As a result, the necessity and demand for IT resources continues to increase.

1 **Q. By how much do you forecast IT Operations and Maintenance (O&M) costs[1] to**

2 **increase?**

3 A. From 2016 to 2018, we forecast IT O&M costs to increase from $57.1 million to

4 $71.6 million as shown in Table 1 below. Because these costs relate to all areas of PGE's

5 operations, they are allocated or charged to appropriate operating areas and appear as part of

6 each area's O&M costs. Since the majority of those costs relate to corporate systems, whose

7 costs are allocated rather than charged directly to the operating areas, we discuss IT as a

8 whole in this testimony.

Table 1
Total IT Costs ($ millions)

Category	2016 Actuals	2018 Forecast	Variance 2018–2016
Direct Charges to Operating Areas	$10.3	$17.3	$7.0
Allocated Charges to Operating Areas	46.8	56.9	10.1
Labor Adjustment	0.0	(0.9)	(0.9)
Other Adjustment	0.0	(1.7)	(1.7)
Subtotal IT Incurred	**57.1**	**71.6**	**14.5**
Labor Loadings Charged to Operating Areas	14.5	21.1	$6.5
Subtotal IT Loaded	**71.6**	**92.7**	**21.1**
2014 IT Deferral Mechanism	1.7	1.7	0.0
Total IT*	**$73.3**	**$94.4**	**$21.1**
FTEs	**272.4**	**316.6**	**44.2**

* May not sum due to rounding

9 **Q. What are the major drivers of this increase?**

10 A. The major drivers are increased support needed for increasingly complex and integrated

11 systems throughout PGE and increased need in the areas of cyber and physical security.

12 **Q. Please explain how IT costs are directly charged or allocated to the specific operating**

13 **areas.**

---

[1] Unless specifically indicated as capital costs, all costs in this testimony refer to O&M costs.

1   A.   As seen in Table 1, PGE's IT costs consist of three categories: directly charged (or

2   assigned), allocated, and labor loadings. Directly charged costs relate to systems that are

3   specific to a given operating area, such as production, transmission, or distribution. These

4   costs are charged directly to specific O&M accounts related to those operating areas. Other

5   IT work in the areas of voice, data, network, communications, business recovery, the data

6   center, and office systems are not directly related to one specific operating area; instead,

7   these costs apply broadly to all PGE activities and departments. These costs are first

8   charged to a balance sheet account and then allocated to the expense accounts for the various

9   operating areas. PGE Exhibit 501 provides the summary by operating area. Labor charged

10   to the balance sheet has associated labor loadings and a corporate governance allocation

11   applied per PGE's loading and allocation policies, which are submitted annually to the

12   Public Utility Commission of Oregon (OPUC) Staff as an attachment to our Affiliated

13   Interest Report.

14   **Q. What do the labor loadings and corporate governance allocations represent?**

15   A.   The labor loadings represent payroll-related costs that are first charged to administrative and

16   general (A&G – e.g., benefits and employee support) and payroll taxes, and then applied to

17   O&M accounts, based on specific rates per allocated IT labor. Ultimately, the costs

18   represented by these loadings begin in O&M and end in O&M so they are not specifically IT

19   costs; rather they are payroll-related costs that follow allocated IT costs.

20   **Q. Why do loadings increase by $6.5 million?**

1   A.   The loadings increase because the labor, on which they are based, is increasing.   Labor is

2   increasing due to escalation and more full time equivalent (FTE)[2] employees.   PGE Exhibit

3   400 provides details regarding the underlying payroll-related costs.

4   **Q.   What does the 2014 IT Deferral Mechanism represent?**

5   A.   As part of the UE 262 settlement process, parties stipulated that 2014 O&M costs associated

6   with developing IT systems should be capitalized and subject to a five-year amortization.

7   The stipulation, subsequently adopted by Commission Order No. 13-459, removed

8   approximately $8.7 million of IT development O&M expense from PGE's 2014 revenue

9   requirement and replaced it with a regulatory asset of approximately $7.8 million, which

10   was included in 2014 rate base. The remaining amortization expense of approximately $1.7

11   million represents one-fifth of the initial capitalized total.

---

[2] FTEs are discussed in Section III.

II.   IT 2020 Vision Update

1   **Q. Please provide a brief summary of the 2020 Vision program.**

2   A.   In UE 215 (PGE Exhibit 600, Section IV, Part B), we described 2020 Vision as a 10-year

3   strategy to "implement a set of projects that collectively modernize and consolidate our

4   technology infrastructure. The ultimate purpose of this program is to replace a multitude of

5   existing software applications with fewer 'enterprise' applications that provide integrated

6   functionality for PGE's operations." In UE 262, we reiterated that the program's goal

7   continues to be to implement common systems and standardized business processes

8   throughout the enterprise to achieve efficiency and cost effectiveness. We also restated that

9   another one of the program's primary objectives is to replace obsolete technologies with

10   new technologies and increased functionality. In Docket No. UE 294, we stated that the last

11   two remaining projects were to replace the current Customer Information and Meter Data

12   Management Systems (expected to close the second quarter of 2018). These projects are

13   part of our Customer Engagement Transformation (CET) program and are discussed in PGE

14   Exhibit 900.

15   **Q. What 2020 Vision projects has PGE successfully implemented to date?**

16   A.   From 2010 through 2016, PGE completed the following 2020 Vision projects:

17   • Work Management System (WMS) Upgrade

18   • Finance and Supply Chain Replacement Project (FSRP)

19   • Infrastructure (hardware) and Program Office

20   • Maximo, Mobile and Scheduling Wave 1 (MMS)

21   • Maximo for IT

22   • MyTime time collection system

1   •   Maximo, Mobile and Scheduling Wave 2

2   •   Geographic Information System (GIS) and Graphic Work Design (GWD)

3   •   Outage Management System (OMS)

4   •   Business Intelligence (BI) Systems

5 **Q. You mention that 2020 Vision is intended to replace numerous applications with fewer**

6 **enterprise systems. How many applications have you retired since 2009?**

7 A. As shown in Table 2 below, by 2018 we will have reduced our number of applications by

8 40% since 2009.

Table 2
Number of PGE Applications

YEAR	TOTAL	% Reduction since 2009
2009	404	
2017	277	(31.4)%
2018	241	(40.3)%

9 **Q. If you have fewer applications to operate and maintain, do they require less support?**

10 A. No. While PGE has significantly reduced the number of applications being supported, on-

11 going support is necessary due to the increased functionality, complexity, and number of

12 interfaces of the new enterprise applications. The increased complexity and need for

13 additional support reflects the new systems having the following:

14   •   Increased functionality/capabilities – For example, the GWD system will provide new

15   functions/capabilities that require incremental FTEs to maintain and support the

16   application on an ongoing basis.

17   •   More interfaces/integration to other systems – For example, Maximo and the Asset

18   and Resource Manager (ARM) scheduler applications have 88 interfaces to/from

1   PeopleSoft Finance, Customer Information System, Field Manager and many other

2   systems; this is compared to approximately 20 interfaces for the legacy Maximo

3   system. The interfaces automate or eliminate the need for clients to manually key

4   information into multiple systems and provides for consistent/common data

5   management. While new interfaces improve efficiency and add functionality, they

6   add complexity because interfaces have the potential for errors, or failed transactions,

7   which becomes another area requiring IT support.

8   • New security policies and regulatory standards/requirements – The more complex

9   systems, especially those with greater scope and capability, introduce further need to

10   protect sensitive or confidential data. PGE must meet more complex standards as

11   specified by Federal Energy Regulatory Commission, North American Electric

12   Reliability Corporation, and other regulatory bodies. It is critical to meet additional

13   security requirements on an ongoing basis.

III.   IT Operations and Maintenance Costs

1   **Q. What are the primary drivers of the increase from 2016 to 2018 related to direct and**

2   **allocated IT charges shown in Table 1 above?**

3   A. The increase is primarily attributable to an increase in labor costs due to the addition of

4   FTEs required to support our growing IT infrastructure. PGE Exhibit 502 provides detailed

5   descriptions of the positions and why they are needed. A breakdown by IT functional area is

6   presented in Table 3 below.

Table 3
Summary of FTE Increase

Area	FTE	Description of Need
Office of CIO	7	To provide support to T&D, infrastructure fitness, software license compliance, expanded/improved IT service delivery, and Western EIM starting in 2017.
Infrastructure	9	To support eastside generation facilities, provide 24/7 IT support in the Data Center, T&D, Customer Service and the Call Center.
Risk	2	Ongoing and expanding support.
Applications	4	Ongoing maintenance and care of new software products.
Information Security Program	22	PGE is further enhancing its cyber security program based on a risk-based prioritization of enterprise-wide cyber initiatives as recommended by outside consultants. This effort is discussed in Section IV below.

7   **Q. What considerations does PGE evaluate when deciding whether to use contractors or**

8   **regular FTEs?**

9   A. Both types of workers have value in our labor strategy. PGE uses contractors in

10   combination with regular FTEs in order to address a number of labor needs, including, but

11   not limited to, short-term assignments, specialized knowledge that is not generally available

12   in our market or at our wage levels, and staffing up for projects that have a finite period and

13   a need for an influx of skilled personnel. Regular FTEs are required to conduct work that is

1 ongoing and integral to our operations, as those operations exist now and into the

2 future.   Regular FTEs need to understand and be able to use and maintain the IT systems

3 that support and protect PGE's operations. We develop our employees with the expectation

4 that they will continue to be part of our IT team, and the time invested creates more value

5 for PGE and for customers.   Further, it can take as many as 160 hours for a contractor to

6 become proficient, which takes time away from other important tasks for the trainers and the

7 contractor. Finally, given the rates that some contractors demand, where new positions

8 replace existing contractors, labor costs decline.

1. Office of the Chief Information Officer (OCIO)

9 **Q. Please describe the seven positions needed for the OCIO.**

10 A. PGE is requesting seven FTEs[3] for the OCIO in order to meet the growing demands of our

11 IT operations. PGE has relied on contractors to do this work in the past but with new

12 systems coming into service that are expected to be integral to our operations, a more stable

13 and reliably available solution is required. Contract employees are generally used on a

14 temporary basis resulting in the need to train new contractors once an existing contractor is

15 no longer engaged in PGE work.

16 **Q.   Why are these positions needed?**

17 A. PGE will need two Western Energy Imbalance Market (Western EIM) positions as we

18 approach our entrance into the Western EIM. Participation in the Western EIM introduces

19 several new applications and interfaces to existing applications that all must be supported to

20 meet the requirements. In addition, Western EIM will operate 24 hours, 7 days a week (i.e.,

21 24/7). The Western EIM is discussed in more detail in PGE Exhibit 300.

---

[3] Described in detail in PGE Exhibit 502

1   To deliver IT service across the organization, we have created two Business Relationship

2   Management analyst positions to help support Transmission & Distribution and Customer

3   Service. These two departments rely significantly on well-functioning IT systems. The

4   more we can work closely with departments and know exactly what they need and why, the

5   better we can serve them.

6   PGE will need three positions to, 1) provide support for ongoing infrastructure fitness

7   evaluation, 2) a software asset manager to monitor compliance with software license

8   agreements, and 3) a Service Level Manager to ensure we continue to provide an

9   appropriate level of service enterprise-wide. The remaining two OCIO positions, which are

10   fully discussed in PGE Exhibit 502, are needed to support our expanding IT systems to

11   maintain and keep the systems operating consistently while minimizing down time.

2.   IT Infrastructure

12   **Q. Please describe the nine new positions in IT Infrastructure.**

13   A. Similar to our need for expanded application support, we are requesting four FTEs to

14   provide 24/7 support at our data center operations. We operate our business 24/7 and it is

15   important that we respond to our employees and customers in a timely manner. For

16   example, customers could be directly impacted if crews are unsure of their next work order

17   due to system constraints. During a major outage, we need our computer systems operating

18   and interfacing to deliver the information needed at the time we need it. As we implement

19   these complex, enterprise-wide applications and integrated systems, 24/7 monitoring is

20   required.

21   In addition, four FTEs are needed to continue providing adequate support to existing and

22   new technologies (i.e., Citrix, Virtual Desktop) and other network equipment that support

1   key applications (i.e., Maximo, OMS, GIS) and interfaces between them. IT is currently

2   limited in the amount of support we provide to these critical systems. The remaining

3   position is for eastside IT support; there are limited qualified contractors available in rural

4   areas and travel time from Portland can be time consuming.

3.   IT Risk Management

5   **Q. Please explain the two positions needed for risk management.**

6   A. The continued expansion and complexity of our systems is driving an increasing need for

7   regulatory and compliance support. The two positions needed for risk management are

8   distributed to two main functions: 1) ongoing administration of PGE's newly developed IT

9   Governance Risk and Compliance (GRC) toolset; and, 2) management of the growing IT

10   Compliance and Disaster Recovery departments. This work is expected to be ongoing and

11   integral to our operations, and therefore it is appropriate for the work to be performed by

12   employees, not contractors.

4.   Applications Support

13   **Q. Please explain why you need four new positions for applications support.**

14   A. As mentioned above, PGE has significantly reduced the number of applications supported

15   by IT, however, these new enterprise applications are far more complex and have greater

16   functionality. Hence, as we expand the functionality of these systems, PGE needs more

17   personnel to provide ongoing support. These positions are to support MMS, GIS, OMS and

18   PeopleSoft. This work is expected to be ongoing and integral to our operations, and is

19   appropriate for the work to be performed by employees, not contractors.

5.   Information Security Program

1 **Q. What progress have you made addressing your Information Security Roadmap since**

2   **your last general rate case?**

3 A. Since our last general rate case, PGE has been developing and evaluating the next steps to

4   our Information Security Roadmap.[4] To assist in that effort, PGE hired outside consultants

5   to perform a comprehensive review of our information security program. One of the

6   primary recommendations by the consultants was a centralized, enterprise-wide security

7   operations center with detailed steps to achieve that goal. PGE also updated its Information

8   Security Roadmap to address the full scope of their recommendations. These initiatives and

9   their implementation are discussed in Section IV below.

6.   Hardware/Software Maintenance Agreements

10 **Q. By how much do software and hardware maintenance agreement costs increase based**

11   **on current planned projects?**

12 A. From 2016 to 2018, these costs will increase by approximately $4.9 million.

13 **Q. Why are software and hardware maintenance agreements necessary?**

14 A. These agreements are necessary to:

15   1) Keep our software operational by having access to fixes and patches

16   provided by the vendor;

17   2) Enable us to obtain and retain appropriate licenses, since some vendors

18   require the purchase of maintenance services as a condition of the software

19   license; and

---

[4] This was previously referred to as the Cyber Security Roadmap but has evolved and been renamed.

1   3)   Receive regular upgrades to correct programming errors and provide

2   continued technical maturity.

3   PGE must provide care and maintenance for our technology investment, which extends

4   the useful life of our systems and provides the best value for customers.

5   **Q.   In previous rate cases, you stated that the 2020 Vision program was intended to replace**

6   **numerous applications with fewer enterprise systems.   If you have fewer systems**

7   **replacing numerous applications, why would PGE's maintenance agreement costs**

8   **increase because of projects such as these?**

9   A.   As we decrease the number of applications through consolidation, we see an increase in the

10   maintenance costs associated with either: 1) new and more effective enterprise applications,

11   or 2) expanded use of existing applications (which is especially pronounced as we replace

12   homegrown software, which requires no maintenance expense other than internal labor to

13   provide support). These expanded and new replacement applications are greater in size and

14   complexity because they are enterprise applications that provide greater functionality than

15   the systems they are replacing, and the maintenance is typically more expensive.

16   **Q.   What are the primary reasons for the increase in hardware and software maintenance**

17   **costs?**

18   A.   O&M costs for maintenance agreements on hardware and software tend to increase annually

19   for the following reasons:

20   •   Price escalation for maintenance services;

21   •   Implementing new applications to meet new or changing requirements; and

22   •   Replacing obsolete systems with more effective systems that deliver greater

23   functionality, but are more complex than the old systems. In such instances, the new

UE 319 – General Rate Case – Direct Testimony

1   systems increase efficiency by eliminating certain manual processes and/or by

2   meeting new requirements that the old system could not address.

3   In other words, increases in the IT operational budget are indicative of purchasing new

4   technologies or expanding the usage of existing technologies. We negotiated maintenance

5   agreements that captured value and we have reduced costs in theses area by volume

6   purchases with a few vendors.

7   **Q. What types of new or expanded systems are you implementing?**

8   A. Examples of new or expanded technologies include:

9   • A new Residential Energy Analysis Program (Opower) as provided by Oracle;

10   • Oracle customer care software for the new CET projects;

11   • New software for hosting the Western EIM system as discussed in PGE Exhibit 400;

12   • An increase in Office 365 (i.e., a cloud version of email) service fees plus additional

13   deployment of Microsoft software. PGE has moved to the cloud because it is the

14   most effective strategy to maximize functionality and speed. Eventually, the only

15   choice will be cloud email services; PGE is following its fellow utilities in making

16   this change;

17   • Increased cyber security monitoring and assessment tools including network analysis,

18   threat monitoring, and security testing and analysis;

19   • Additional investments in outside vendors, such as Gigamon and NetScout[5], for

20   systems and network monitoring;

---

[5] Gigamon is a technology vendor that provides network visibility and traffic monitoring. NetScout provides application and network performance management products.

1   • Planned expansion of process intelligence (PI) software[6] for energy asset monitoring

2   and analysis;

3   • Increased deployment of our security event and incident management tool; and

4   • New software to support better internal control monitoring.

5   **Q.   What are other sources of cost increases from 2016 to 2018?**

6   A.   Increases in non-labor costs are due to hardware/software maintenance agreements, which

7   are becoming numerous, and use of contractors or outside services. PGE will still have to

8   rely on contractors for some of the work that we have planned during 2017 and 2018. We

9   emphasize the great complexity of supporting our new systems and the need to protect those

10   systems from numerous cyber threats experienced daily by individuals, corporations, and

11   governments. The threat is real and must be addressed, which will require both labor

12   and non-labor support. Contract labor may have been appropriate in previous years as we

13   built our system. Now that these systems are coming online, it is appropriate for regular

14   employees to learn the systems and support them going forward. Although contract labor is

15   increasing, it would have been greater if not for the shift to regular FTEs.

---

[6] Process intelligence software can help an organization improve process management by monitoring and analyzing processes on a historic or real-time basis. Process intelligence uses data that has been systematically collected to analyze the individual steps within a business process or operational workflow.

IV. Information Security Program

1   **Q. How is PGE addressing the increasing threats related to cyber security?**

2   A.   During 2016, PGE conducted an external review of its Information Security Program (ISP).

3   While PGE had spent significant effort and expense in increasing its security capabilities in

4   recent years, the intent was to ensure that PGE was keeping abreast of increasing cyber

5   threats and corresponding best practices to prevent those threats from circumventing PGE

6   systems. PGE works with many outside parties including other utilities, third-party security

7   experts, industry security groups and others to monitor threats to the electric sector. We are

8   concerned with the increase in scope and severity of recent cyber-attacks on America's

9   critical electronic networks and it is necessary that we take steps now to maintain the

10   security, reliability, and safety of our systems. It is PGE's responsibility to protect the

11   security of our computers, control systems, and other cyber assets that help operate the grid

12   from cyber vulnerabilities.

13 **Q. Isn't PGE already responding to cyber security threats?**

14 A.   Yes. PGE has a rigorous program in place to protect critical infrastructure. Our primary

15   focus has been on corporate systems, such as financial and customer systems, as this was

16   where attacks were targeted in the past. However, we are seeing a significant shift in the

17   industry. Operational Technologies (OT),[7] SCADA systems, substation equipment and

18   generating plants are quickly becoming potential targets as threats become more

19   sophisticated and complex. Attacks are frequently occurring when system monitoring is at

20   its lowest, such as nights and weekends. It is becoming even more critical to protect the

---

[7] OT refers to operational technology or the use of computers to detect or cause a change through the direct monitoring and/or control of physical devices, process and events in the enterprise. http://www.gartner.com/it-glossary/operational-technology-ot/

1   safety of our system from exploitation, compromise, or attack (both physical locations and

2   electronic breaches) as our system relies more and more on technology. PGE's current

3   program needs to expand its focus to equally protect OT systems and do so on a 24/7 basis.

4   **Q. Please provide some examples of threats that may impact PGE operations.**

5   A. The following two examples serve to emphasize the nature of these threats:

6   • A recent cyber security incident in Ukraine[8] points to, 1) the need for vigilance and

7   awareness among all users to prevent social engineering threats; 2) the importance of

8   securing OT networks; and 3) the importance of 24-hour monitoring of critical

9   networks.[9]

10   • National Public Radio featured a story in October[10] about a corporation that

11   experienced a major, complex hacking attack commonly referred to as "distributed

12   denial of service" attack, and security experts see these kinds of attacks all the time.

13   They happen when hackers take over several computers and infect them with

14   malicious software and then use them to barrage a website or a web service with fake

15   traffic until the website/web service stops functioning under this overwhelming

16   demand. This type of attack points to, 1) the creativity with which attackers exploit

17   new technology; 2) the need to not just consider conventional "IT" networks but also

18   non-traditional operational technology devices; and 3) again, the need for 24/7

19   monitoring.

---

[8] http://abcnews.go.com/International/ukraine-conflict-monitor-osce-confirms-cyber-attack/story?id=44430311
[9] Threats can lurk undetected for weeks or months and then suddenly be deployed in a brief period of time.
[10] http://www.npr.org/2016/10/22/498954197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popula

1　Q.　**What were the results of this review?**

2　A.　The review affirmed the many things PGE is doing correctly and identified additional

3　　　security measures to address by successfully executing certain multi-year, enterprise-wide

4　　　cyber security initiatives.　After analyzing these gaps, PGE incorporated these

5　　　recommendations into our existing multi-year Information Security Roadmap to address the

6　　　findings of the study that includes several initiatives.　Each of these initiatives makes up a

7　　　series of projects to achieve the full value of the initiative.　Projects are a blend of capital

8　　　assets and operating improvements.

9　Q.　**When will PGE implement these initiatives?**

10　A.　The primary implementation of these initiatives will begin in 2017 and continue through

11　　　2021.

12　Q.　**Please briefly describe these initiatives.**

13　A.　Based on the potential impact of identified risks, PGE identified the following ten key

14　　　initiatives:

15　　　　• Integrated Security Operations Center (ISOC) – Execute a multi-phase initiative to

16　　　　　perform proper analysis, planning and coordination to determine the appropriate

17　　　　　scope and maturity level for the capabilities of an enterprise-wide ISOC.

18　　　　• Identity and Access Management (IAM) – Improve PGE's identity and access

19　　　　　management governance including processes and tools to establish, extend or

20　　　　　improve key service capabilities across the enterprise including user access lifecycle

21　　　　　management, access management, and use of role-based access controls.

22　　　　• Risk Based Governance – Improve executive leadership's control and visibility into

23　　　　　enterprise-wide cybersecurity risks in order to comprehensively manage cyber threats

1   to acceptable tolerance levels. Strengthen partnership through jointly defined roles

2   and responsibilities for collaboration and decision making involving executive

3   management.

4   • Incident Response – Define and develop an enterprise-wide incident response process

5   and plan to efficiently and effectively respond to future potential incidents.

6   • Business Impact Analysis (BIA) – Perform planning to update previous processes and

7   procedures to assess and prioritize critical PGE business functions and processes

8   based on the identification of potential business interruption risks and impacts.

9   • Vendor third-party management – Enhance relationship between security and

10   procurement by applying security focused, risk-based vendor/third-party management

11   concepts at each stage of the vendor/third-party management lifecycle.

12   • Architecture – Plan for and implement a security architecture function across PGE.

13   • Vulnerability Management – Develop comprehensive vulnerability management

14   program that covers all assets and adequately detects and reports vulnerabilities in

15   PGE assets to best identify risk.

16   • Security Awareness and Training – Strengthen and enhance an enterprise-wide

17   security awareness program for all employees, and conduct targeted training for

18   security staff.

19   • Data Protection – Enhance existing data classification and data protection policies

20   and implement an enforcement mechanism to strengthen data loss prevention.

21   The list above is not presented in any specific order. Each initiative represents multiple

22   projects that align with one or more of the study's recommendations and PGE's goals.

1   **Q. What activities does PGE plan during 2017 and 2018 to support the initiatives?**

2   A.   PGE's 2017/2018 plans include multiple initiatives as identified by PGE and the study.

3   These initiatives are designed to: 1) establish appropriate governance, policies, procedures,

4   and processes to support effective investment in security tools; and, 2) follow-up with

5   design and development of assets required to support those processes.

6   The majority of 2017 work includes the design and initial development stages of a 24/7

7   ISOC, and the development of an IAM solution set. Other activities include process

8   enhancements and staffing to support improved third-party risk management, security

9   architecture and design, and incident response.

10   In 2018, activities focus on the completion of the ISOC and continued phased

11   deployment of IAM solutions, including expansion into field technologies and Role-Based

12   Access Control (RBAC).

13   **Q. How many FTEs will you require in 2017 and 2018 for these activities?**

14   A.   PGE is expecting to hire 22 FTEs during 2017 and 2018. PGE Exhibit 502 describes the

15   FTEs in detail.

16   **Q. Please explain why you need 22 FTE to implement the ISP.**

17   A.   PGE has evaluated the labor efforts and support required to implement the necessary

18   security initiatives at 22 FTEs. The ISOC will be staffed 24/7 and will require nine FTEs.

19   Their function will be to perform security monitoring, system administration, configuration,

20   event response, threat response and incident response on an enterprise-wide basis. The

21   impact of security threats is no longer just for basic IT systems, but must expand to cover

22   the entire enterprise.

1   Five FTEs are required to implement IAM, a key initiative, which will help improve and

2   maintain PGE's identity and access management governance, including processes and tools

3   to establish, extend or improve key service capabilities across the enterprise. With all the

4   new applications and software being implemented, security and authorized access needs to

5   be established. In parallel, we will be implementing additional controls such as automated

6   password vaulting, rotation, and monitoring to high risk accounts.

7   We are increasing four FTEs for security testing, third-party risk management, threat

8   analysis, and design architecture to ensure the integrity of our systems.   The security

9   breaches that occurred at both Target[11] and Home Depot[12] involved third-party (vendors)

10   access to systems. In addition, two FTEs (one manager, one administrative) are needed to

11   supervise compliance, security, operations and strategic planning personnel. This

12   consolidates employees critical to security efforts into one department. The remaining two

13   FTEs focus on overseeing the overall implementation of the Information Security Roadmap,

14   which consists of roughly 40 projects over five years.

---

[11] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[12] https://www.infosecurity-magazine.com/news/home-depot-breach-third-party/

V. Qualifications

1   **Q. Mr. Henderson, please provide your qualifications.**

2   A. As Vice President of PGE for Information Technology, I am responsible for the

3   infrastructure, operations and system development of all information systems. This includes

4   developing a strategic plan for information technology and implementing enhanced project

5   management and methodology. I joined PGE in 2005 after serving as Chief Information

6   Officer at Stockamp & Associates since 2003. Previously, I spent eight years as senior

7   IT manager for Willamette Industries, Inc. and was Vice President and Chief Information

8   Officer for four years. I received a bachelor's degree in management from Harding

9   University in Searcy, Ark., and an MBA from the University of Texas. I am also a Certified

10   Public Accountant in Oregon (inactive status).

11   **Q. Mr. Hosseini, please provide your qualifications.**

12   A. I earned a Bachelor's degree in Finance and MBA from Portland State University, where I

13   teach courses in Management, Finance, and Information Technology. I have also taught

14   Management and Human Resources courses for the University of Phoenix and the Utility

15   Management Certificate course for Willamette University. I currently work as the Director

16   of the Office of the Chief Information Officer. Prior to this, I held leadership positions in

17   the Human Resources, Organizational Development, Finance and Accounting, Business

18   Decision Support, and Distribution departments at PGE. Additional experience includes

19   retail sales management, restaurant management, as well as consulting work for a variety of

20   clients.

1 **Q. Mr. Anderson, please provide your qualifications.**

2 A. As Director of Information Security, I am responsible for management and direction of

3 PGE's Information Security Program and the operational oversight of its Information Risk

4 Management department including security assurance, IT CIP Operations, disaster recovery

5 and compliance functions. This includes the responsibility for securing all PGE technology

6 based assets and environments and working with other experts in the security field to design

7 and support industry best practices. I earned a Bachelor's degree in Information Systems

8 from Utah State. My extensive background in security, compliance and risk management

9 have supported the continuing evolution of security practices at PGE. I have more than 20

10 years of security experience and maintain numerous industry certifications in security

11 management, risk management, forensics, auditing and various technical functions.

12 **Q. Does this conclude your testimony?**

13 A. Yes.

List of Exhibits

PGE Exhibit	**Description**
501	Summary of IT Costs by Operating Area
502	IT FTEs - Description of Need

IT Summary by Operating Area

Function	2014 Actuals	2015 Actuals	2016 Actuals	2017 Budget	2018 Forecast	2018-2016 Delta	Annual % Delta 2018-2016
Production							
Assigned	333,366	264	254	-	-	(254)	-100.0%
Allocated	6,695,618	7,264,124	9,557,999	8,827,113	11,069,073	1,511,074	7.6%
Assigned Adjustments					(353,906)	(353,906)	
IT Deferral	(1,251,885)	312,972	312,972	312,971	312,971	(0)	
Total Production	5,777,098	7,577,359	9,871,224	9,140,084	11,028,138	1,156,914	5.7%
Power Operations							
Assigned	462,192	1,022,349	1,011,868	1,617,246	2,164,340	1,152,472	46.3%
Allocated	1,610,682	1,772,266	1,492,874	1,150,370	1,439,973	(52,901)	-1.8%
Assigned Adjustments					-	-	
IT Deferral	-	-	-	-	-	-	
Total Power Ops	2,072,875	2,794,615	2,504,742	2,767,616	3,604,313	1,099,571	20.0%
Transmission							
Assigned	323,714	301,316	595,346	807,480	935,139	339,792	25.3%
Allocated	1,415,835	1,470,604	1,407,217	1,168,727	1,462,951	55,734	2.0%
Assigned Adjustments					(39,761)	(39,761)	
IT Deferral	(224,394)	56,099	56,099	56,099	56,099	0	
Total Transmission	1,515,155	1,828,018	2,058,662	2,032,305	2,414,427	355,765	8.3%
Distribution							
Assigned	732,596	981,509	3,388,577	3,728,055	4,564,270	1,175,693	16.1%
Allocated	16,563,746	17,722,661	20,826,809	23,252,158	29,105,827	8,279,018	18.2%
Assigned Adjustments					(525,650)	(525,650)	
IT Deferral	(1,661,770)	415,443	415,443	415,443	415,443	0	
Total Distribution	15,634,572	19,119,613	24,630,829	27,395,656	33,559,890	8,929,062	16.7%
Customer Acctg/Svc							
Assigned	2,518,166	3,742,323	2,751,874	4,196,604	7,536,379	4,784,505	65.5%
Allocated	13,321,027	13,434,747	14,072,169	14,104,269	17,654,982	3,582,814	12.0%
Assigned Adjustments					(509,012)	(509,012)	
IT Deferral	(2,109,865)	527,466	527,466	527,466	527,466	(0)	
Total Customer Acctg/Svc	13,729,329	17,704,536	17,351,509	18,828,339	25,209,815	7,858,306	20.5%
A&G							
Assigned	4,358,145	4,622,875	4,523,496	5,140,231	5,536,900	1,013,404	10.6%
Allocated	9,774,225	10,565,799	11,975,293	11,056,225	13,771,155	1,795,863	7.2%
Assigned Adjustments					(289,305)	(289,305)	
IT Deferral	(1,699,285)	424,821	424,821	424,821	424,821	(0)	
Total A&G	12,433,086	15,613,495	16,923,610	16,621,277	19,443,571	2,519,961	7.2%
Totals							
Assigned	8,728,180	10,670,636	12,271,415	15,489,616	20,737,027	8,465,612	30.0%
Allocated	49,381,133	52,230,200	59,332,360	59,558,861	74,503,961	15,171,601	12.1%
Assigned Adjustments	-	-	-	-	(1,717,634)	(1,717,634)	
IT Deferral	(6,947,200)	1,736,800	1,736,800	1,736,800	1,736,800	(0)	
Totals by Operating Area	51,162,113	64,637,636	73,340,575	76,785,277	95,260,154	21,919,579	14.0%
Labor Adjustment				(839,747)	(863,355)		
Adjusted Grand Total	51,162,113	64,637,636	73,340,575	75,945,530	94,396,799	21,056,224	13.5%
Control		-	-	-	-	-	

Title	FTE	2016-2018 Incremental FTE – Description of Need
IT - GENERAL		
Office of Chief Information Officer (OCIO)		
IT Business Relationship Management Analyst – T&D	1	Analyst to support T&Ds planning and execution of IT initiatives. Includes roadmap development, project proposals and intake, and issue resolution. The technology needs across T&D continue to grow each year. Aligning all of this work with IT, prioritizing, ensuring timely issue resolution are all critical to the successful implementation and support of T&Ds technology solutions. Work has been allocated across multiple resources, but this is causing growing priority and alignment issues.
IT Business Relationship Management Analyst, Customer Service and Delivery	1	Analyst to support Customer Service and Delivery planning and execution of IT initiatives. Includes roadmap development, project proposals and intake, and issue resolution. The demand for new technology that supports our customer's needs continues to grow each year. Aligning this work with IT, prioritizing, ensuring timely issue resolution are all critical to the successful implementation and support of our customers.
Business Analyst	1	Support the ongoing Infrastructure Fitness evaluation for replacement and growth of infrastructure equipment used to support IT systems. Currently we fill this position with a contractor and since this is an ongoing project the cost to the company would be less if filled with an FTE.
Software Asset Manager	1	Responsible for reviewing and maintaining software license compliance over the IT portfolio. A dedicated resource to review and coordinate compliance will reduce the risk of compliance issues moving forward and license and maintenance optimization may further reduce IT maintenance expenses. Today this role is spread across all IT operating functions which complicates compliance activities, increases compliance risk and increases license compliance costs.
Service Level Manager	1	Responsible for managing IT Service Levels and Continuous Service Improvement. As the IT organization transitions from a technology provider to a service provider additional emphasis is required to identify, measure and improve service delivery.

Analyst, Business and Design, EIM	2	Entrance into the EIM introduces several new applications and new interfaces to existing applications. The large addition of new software solutions increases the support load required from the OCIO IT Energy Systems team. To meet this increased demand an additional Business Analyst and Developer Analyst are required. Many of the new applications require 24/7 support. This high availability will require the IT Energy Systems team to cover more systems during the usual off hours placing greater strain on capabilities of a relatively small team.
Infrastructure		
Specialist IV, Technical	1	Support for eastside generation facilities to perform technical support. There is currently less on-site support for generation sites on the eastside. Given the distance from Portland, techs are only sent out as needed or on infrequent rotation leaving a gap. Contractors have been considered, but adequately trained individuals are difficult to find in rural locations. This will be a long-term, ongoing need.
System Analyst III, 24/7 Operations in Data Center	4	The requirements for 24/7 support of our data center is driven by high availability requirements of (2020 Vision) key line of business application implementation that are highly integrated and automated across various IT systems. If systems go down on the weekend or in the middle of the night, IT needs to be available immediately to help resolve the issue, especially if this occurs during an outage event, which could directly impact customers.
System Analyst III, Citrix Support	1	PGE's Outage Management System and virtual desktop architecture for our call center are delivered from a Citrix environment. Infrastructure team currently is limited in number of FTE to provide adequate Citrix support to the business.
System Analyst IV, TCC IVT Support	1	To provide adequate support of PGE's Call Center Technology additional Cisco Networking expertise is required. This is mainly driven by a very complex and integrated solution stack that is comprised of several technology domain.
Specialist	1	Provides support for IT Infrastructure. Increased number of critical applications that require faster response to infrastructure issues (i.e., OMS, GIS, Maximo). Additional staff needed to increase on-site staffing model beyond 40 hours per week, and provide more resources to respond to issues after normal business hours.
Design Build Specialist	1	Increased complexity of systems and the need to automate more of the build process. Many architecture design enhancements not covered by capital projects requiring more O&M resources. It is critical to have core resources that are knowledgeable about the PGE IT environment.

Applications		
IT Systems Manager	1	We have invested in several new software products to support cyber security and IT operations. The ongoing maintenance and care of these systems needs to be treated like other software products used by the business. The approach that we have used successfully in the past has been to devote a team dedicated to that line of business to maintain these systems. With the implementation of several new systems in this area, we believe we now have enough work that requires a dedicated team to support them. Most of the people in this team are being reassigned from other teams. The only net new person is a manager to oversee this group.
Quality Assurance Analyst	2	Required to provide quality assurance support for Business Intelligence, GIS, Finance, and Human Resources. The applications supported are complex and require highly skilled QA analysts.
Quality Assurance, Release Manager	1	This position is required to provide Release and Deployment support for IT Applications project and team efforts, currently supported by a mix of both FTE and contractors. Current and future workloads make it clear that present staffing levels will be inadequate to provide the necessary level of accuracy and completeness that Release involvement delivers to the enterprise.
Risk		
Governance Risk Compliance System Support	1	Currently, there are no FTEs assigned to support and administer the GRC tool. When GRC was deployed in 2015, it was expected that support needs would be minimal. However, based on volume of regulatory changes and enhancements in the last 18 months, and the other uses for the tool, PGE has reassessed its need. This position will provide services that are not currently being performed and will reduce the overall vendor spend for the support of the applications. The GRC tool provides increase automation and notification of compliance requirements and workflows.
Compliance Manager	1	Management over the growing IT compliance and disaster recovery departments. This manager will oversee 5-8 FTE plus 2-3 contingent workers. Provide increased oversight on IT compliance and risk directives.
TOTAL IT FTEs	**22**	

INFORMATION SECURITY PROGRAM		
Security Assurance		
ANALYST IV,SR Information Security	2	These roles will provide security testing of PGE systems traditionally performed by contractors to ensure PGE systems are configured and maintained in a secure fashion. Contractor testing is less efficient and more costly than internal staff. This work has been performed by 4-5 contractors.
Analyst IV, Security Assurance	1	This analyst will perform third-party risk management, contracts and vendor testing.
Analyst IV, Threat Analyst	1	This role develops and performs the threat management function. He/she focuses on the identification, analysis and response to new and emerging threats.
Information Security Operations Center (ISOC)		
Manager, ISOC	1	New manager identified by outside consultant study for newly defined team based on executive request for enterprise security operations group to be developed.
Analyst, ISOC	5	Staff of newly identified and newly developed 24/7 ISOC. ISOC functions to include security monitoring, system administration, configuration, event response, threat response and incident response. ISOC coverage to expand from basic IT to enterprise IT and OT.
Spec V, Security Monitoring	1	This role serves as liaison and support between corporate security and cyber security as it relates to 24/7 Incident Response as part of new ISOC.
Specialist, ISOC, T&D	2	Staff of newly identified and newly developed 24/7 ISOC. ISOC functions to include security monitoring, system administration, configuration, event response, threat response and incident response. ISOC coverage to expand from basic IT to enterprise IT and Operational Technologies (OT). Specialist focused and trained on T&D OT systems.

Identity Access Management (IAM)		
Analyst IV, Applications Developer	2	Combined developers, administrator and quality assurance analysts assigned to the development, support, administration and code testing for Password Vault, IAM, and other access tools.
Analyst IV, Role Manager, RBAC	1	Process manager required to design, develop and support ongoing Role Based Access Control, permissions and governance.
Analyst IV, Governance, Access & Reporting	1	Compliance Analyst required to support ongoing access governance, reporting and system design for multiple regulations including SOX, CIP and HIPAA
Analyst III, Identity/Access Bus Analyst	1	Analyst to support the planning, design, requirements and documentation of projects associated with capital investment. (roughly 14 projects over 5 years)
Information Security Roadmap		
Program Manager, ISP	1	Program Manager will lead/facilitate the design, development and implementation of this multi-year information security program roadmap. Oversee budgets, planning, schedules and multiple project managers.
Analyst IV, Program Bus Analyst	1	Analyst to support the design, requirements and documentation management of roadmap projects not associated with capital investment (roughly 40 projects over 5 years)
T&D/Security		
Manager, T&D OT Support Services	1	Manager to supervise compliance, security, operations and strategic planning personnel. This consolidates employees critical to security efforts into one department and allows the General Manager to dedicate 25% of time to Security leadership.
Admin, T&D Substation Support	1	Admin assistant to coordinate documentation, meetings, manager schedules and action items associated with Security efforts. This additional support ensures the General Manager of Substation OT is able to dedicate 25% of time to Security leadership.
Total ISP FTEs	**22**	
Total IT FTEs	**44**	