www.pse.com

PUGET SOUND ENERGY
The Energy To Do Great Things

Puget Sound Energy, Inc.
P.O. Box 97034
Bellevue, WA 98009-9734

September 19, 2014

Mr. Steven V. King, Executive Director and Secretary
Washington Utilities and Transportation Commission
P.O. Box 47250
Olympia, Washington 98504-7250

Re: Docket Nos. UE-072300 and UG-072301
2013 PSE Critical Infrastructure Security Annual Report – Filed Electronically

Dear Mr. King:

Per the informal data request of the Commission staff on July 29, 2014, Puget Sound Energy, Inc. ("PSE") respectfully submits its 2013 PSE Critical Infrastructure Security Annual Report. Please note that PSE has already voluntarily included its 2013 Cybersecurity Reporting as Attachment C to its 2013 SQ Program and Electric Service Reliability Filing on March 28, 2014.

Please contact Eileen Figone at Eileen.Figone@pse.com or (425) 456-2680 or Eric Englert at Eric.Englert@pse.com or (425) 456-2312 for additional information about this filing. If you have any other questions please contact me at (425) 456-2110.

Sincerely,

Ken Johnson
Director, State Regulatory Affairs

Enclosure

2013 PSE Critical Infrastructure Security Annual Report

Puget Sound Energy (PSE) puts a strong focus on cybersecurity and physical security. PSE's goal is to apply the same level of due diligence across the enterprise – which includes critical infrastructure – to ensure a consistent approach to security is maintained no matter the program. All security program activities and results are treated as highly sensitive and confidential so as not to increase risk to the company through the exposure of known vulnerabilities or potential threats. However, PSE looks forward to providing a detailed briefing in a confidential meeting with the Washington Utilities and Transportation Commission.

Organizational

The Information Security & Risk organization (focusing on cybersecurity) was restructured in early 2013 to provide more focus on security strategy and the aligned programs for improving PSE's cybersecurity posture. Ultimately, this approach simultaneously prioritizes the work according to the highest risk threats and continues the construction of an ever-evolving cybersecurity program to protect PSE and the cyber risks it faces.

The team has the following roles and resources:

- Manager/Information Security Officer (1)
- Security Architect (1)
- Advisor IT Security Analyst (4)
- Senior IT Security Analyst (5)
- Senior Records Management Analyst (2)
- Administrative Specialist (1)

Some of the aligned cybersecurity programs are:

- Security Assessment Program – processes that ensure technology implementations meet set security controls around data management, disaster recovery, compliance, secure coding, contract requirements, etc.
- Incident Response Program – processes that ensure appropriate measures are followed when investigating, reporting, and remediating a cybersecurity incident.
- Records Information Management Program – processes that ensure appropriate management is applied to all company records
- Vulnerability Management Program – processes that ensure activities such as vulnerability assessments and secure code reviews are performed in support of security activities (e.g. security assessments, system patching, etc.).
- Disaster Recovery Program – processes that ensure appropriate business processes and their aligned technologies are available per the determined recovery time objectives.

The restructure was also an opportunity to right-size span of control to improve employee/manager ratio and better consolidate similar functions and processes to create consistency and leverage resources more efficiently.

The Corporate Security team (focusing on physical security) has the following roles and resources:

- Manager (1)
- Administrative Assistant (1)

- Sr. Regulatory Compliance Analyst (1)
- Investigator (2)
- Physical Security Systems Administrator (2)
- Security Systems Technician (1)

There have not been any changes to the organizational structure or placement of the Corporate Security team during 2013.

Risk Assessments

There are a variety of national and industry oriented cybersecurity and physical security risk assessment processes and tools. Since each process and/or tool approaches cybersecurity and physical security from a slightly different perspective, PSE pulls from multiple sources to ensure a more well-rounded view into the security activities needed to lower or mitigate risks.

Vulnerability Management – Activities and Actions

The Vulnerability Management program ensures activities such as vulnerability assessments and secure code reviews are performed in support of cybersecurity activities (e.g. security assessments, system patching, etc.). All results are documented and tracked on a risk register for follow-up and remediation.

Incident Support and Response

Puget Sound Energy participates in the Edison Electric Institute Spare Transformer Equipment Program (STEP) and has been since 2006.

Puget Sound Energy has an Incident Response Plan (Cyber Security Incident Response Plan - CSIRP). The Incident Response Plan was last updated on October 9th, 2013, is tested at least annually.

Security Policies

Cybersecurity Policy – Outlines framework for the identification and protection of Cyber Assets and Critical Cyber Assets subject to the NERC CIP Cyber Security Standards.

Information security policy – Outlines expectations regarding the protection of PSE data as well as any system that stores, processes, or transmits PSE data via appropriate data classification.

Password standard – Outlines password requirements for individual and system accounts. An updated password standard was published in 2013 to better align with technology capabilities.

Physical security policy – Outlines physical security procedures at PSE facilities for employees and contractors.

Records information management policy – Newly created policy that outlines the process and procedures for managing the entire life cycle of company records from creation, active use, inactive storage, and disposal or preservation.

There are also a variety of additional PSE policies that support security best practices but are not specifically driven by security (e.g. electronic messaging and communication policy).

Cybersecurity and Physical Security Budgets

The cybersecurity and physical security budget is in alignment with the security activities identified in the security roadmap.

Collaboration Efforts

PSE participates in a variety of industry and local cybersecurity or physical security offerings and information sharing events. Some of the industry offerings PSE has utilized and participated in including (but are not limited to) the following:

- American Gas Association Security Group
- Edison Electric Institute Security Group
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- FBI Cyber Task Force's FLASH Alerts (FBI FLASH Alerts)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Western Electricity Coordinating Council Physical Security Group
- Critical Infrastructure Protection Physical Security Working Group
- King County Critical Infrastructure Protection Work Group
- Public, Regional Information Security Event Management (PRISEM)
- Washington Fusion Center

PSE also participated in the following local events:

- Visited Western Electricity Coordinating Council (WECC) in the fourth quarter of 2013 to build a stronger partnership and further open the doors of communication. During the visit, PSE reviewed the changes to the various PSE departments that participate in North American Electric Reliability Council Critical Infrastructure Protection (NERC CIP) compliance. There were also discussions of what was working well in the interaction of the two organizations and the opportunities for improvement.

- Attended Cyber Storm Evergreen exercise sponsored by the Washington Military Department to learn more about the exercise for future participation.

- Participated in planning and panel discussion at the Cyber Summit 2. The summit was sponsored by Pacific Northwest National Laboratory, PSE, Snohomish PUD, Tacoma Public Utilities, University of Washington Tacoma, and Washington Utilities and Transportation Commission. The summit was held on April 17, 2014, and included topics such as an overview of cybersecurity in 2014, lessons learned from cybersecurity exercises performed in 2013, and breakout sessions to discuss how the stakeholders in Washington can best work together in response to cybersecurity events.

2013 Cybersecurity and Physical Security Events

PSE did not have any cybersecurity or physical security events in 2013 that resulted in a loss of service, exposure of sensitive customer data, serious financial harm nor required involvement or reporting to the Federal Bureau of Investigation, Department of Homeland Security, military, law enforcement or another regulatory body.