Docket Nos. UE-072300 and UG-072301

Puget Sound Energy
2013 SQ Program and Electric Service Reliability Filing

Attachment C:
2013 PSE Cybersecurity Reporting

PUGET SOUND ENERGY

2013 PSE Cybersecurity Information Reporting

Standard Practices

Updates to cybersecurity policies and/or organizational structure

Organizational

The Information Security & Risk organization has been restructured to provide more focus on Security strategy and the aligned programs for improving PSE's security posture.

Some of the aligned 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 cyber 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.

It 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.

Cybersecurity Policies

A new records information management corporate policy has been created and submitted for approval. The new policy outlines the process and procedures for managing the entire life cycle of company records from creation, active use, inactive storage, and disposal or preservation.

An updated password standard was published to better align with technology capabilities.

Cybersecurity Budgets

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

Vulnerability Management – Activities and Actions

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

Collaboration Efforts

- Compliance team members visited Western Electricity Coordinating Council (WECC) in the fourth quarter of 2013 to build a stronger partnership and further open the doors of

communication. We covered changes to the various PSE departments that participate in North American Electric Reliability Council Critical Infrastructure Protection (NERC CIP) compliance and discussed what was working well in our interactions for both organizations and where we saw opportunities.

- Information Security & Risk team members attended Cyber Storm Evergreen exercise sponsored by the Washington Military Department to learn more about the exercise for future participation.
- Participated in planning Cyber Summit 2 with local utilities and government bodies. The 'summit' is scheduled for April 17, 2014 and will include topics such as an overview of cybersecurity in 2014, lessons learned from cybersecurity exercises performed in 2013, and breakout sessions to discuss how our state can best work together in response to cybersecurity events.

Mandatory and voluntary compliance status regarding federal and state standards:
Successfully completed 2013 NERC CIP self-certification on February 28, 2014.

2013 Cyber Events

PSE did not have any cyber 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.