Puget Sound Energy

2014

Critical Infrastructure Security Annual Report

Filed on March 27, 2015

PSE PUGET SOUND ENERGY

CONTENTS

CRITICAL INFRASTRUCTURE SECURITY 2014 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.

1.1 CRITICAL INFRASTRUCTURE SECURITY – CYBERSECURITY AND PHYSICAL SECURITY

1.1.1 Critical Infrastructure Security Policy and Teams

1.1.1.1 Critical Infrastructure Security Policy

Please provide a copy of the company'sCritical Infrastructure ("CI") Security policy. In subsequent reports, please provide copies of any sections of the policy that have been added or modified since the last report.

The overall PSE cybersecurity policy has not changed in 2014.

The overall PSE physical security policy has not changed in 2014.

1.1.1.2 Critical Infrastructure Security Team

Please provide an organizational diagram of the company's CI Security team(s). The diagram, or accompanying list, should include the names and titles of staff on the team, including any vacant positions or staff in acting roles.

The cybersecurity team did not change in 2014.

The roles and resources are as follow:

- 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)

The physical security team did not change in 2014.

The roles and resources are as follow:

- Manager(1)
- Senior Investiagtor (2)
- Physical Security Program Administrator (1)

- Senior Regulatory Compliance Analyst (1)
- Security Technician (1)
- Administrative Specialist (1)

1.1.2 Critical Infrastructure Security Policy and Teams Changes

1.1.2.1 Critical Infrastructure Security Policy Changes

Please provide a written description of any changes made in the past year to the company's CI Security policy, and any changes to the team structure or the placement of the team in the company's organizational structure.

There have been no changes to PSE's physical security and cybersecurity policies in 2014.

1.1.2.2 Critical Infrastructure Security Team Changes

Please provide a written description of any changes made in the past year to the company's CI Security policy, and any changes to the team structure or the placement of the team in the company's organizational structure.

There have been no changes to the PSE physical security and cybersecurity teams in 2014.

1.1.3 PSE's External Participation

Please describe the company's participation in regional or national tabletop exercises, conferences, committees, or other events related to CI Security.

FERC Cybersecurity Technical Conference – Nationally represented utilities, government bodies, and technology vendors met to discuss data protection and how/if data protection guidelines should be included in NERC CIP requirements.

FERC/PSE Meeting – Private meeting to discuss cybersecurity and physical security priorities and opportunities for PSE and FERC to work together.

FBI – PSE meeting with local FBI resources to discuss current cybersecurity and physical security threats and concerns and to establish our on-going relationship.

CyberSummit – Cybersecurity conference with local utilities and government bodies. Topics included an overview of cybersecurity in 2014, lessons learned from cybersecurity exercises performed in 2013, and breakout sessions to discuss how Washington state can work collaboratively in response to cybersecurity events.

Building Cyber Defense Alliances – Cybersecurity conference hosted by the Bonneville Power Administration focused on insights from subject matter experts in the field of cyber security, sharing of lessons learned for continuous improvement, the latest on current threat information, and building relationships with other utilities and government bodies in the Pacific Northwest.

DHS-EEI Physical Security Awareness Campaign – Inter-agency campaign designed to raise awareness and provide public, private, and law enforcement communities resources to enhance the physical security and resilience of electric substations.

PSE is also an active participant in many events related to Critical Infrastructure Security. Below is a list of committee's PSE participated in during 2014.

- WECC CIPUG
- American Gas Association Security Group
- Edison Electric Institute Security Group
- Western Electricity Coordinating Council Physical Security Group
- Critical Infrastructure Protection Physical Security Working Group
- King County Critical Infrastructure Protection Work Group
- Washington Fusion Center

1.1.4 Unauthorized actions related to cybersecurity and physical security

Please include a list of any unauthorized actions related to cybersecurity and physical security that have occurred since the last report which led to one or more of the following:

i. *loss of service;*
ii. *interruption of a critical business process;*
iii. *breach of sensitive business or customer information;*
iv. *or serious financial harm.*

PSE did not have any cybersecurity or physical security events in 2014 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.

1.1.5 Incident Response

Does the company have retainers or contracts for outside help in the event of an incident?

PSE currently does not have a retainer or contract for cybersecurity or for physical security support in the event of an incident, however this is under consideration.

What kind of support is provided by the company's incident response retainers or contracts that provide similar services?

PSE currently does not have a retainer or contract for cybersecurity or for physical security support in the event of an incident.

Is the company currently participating in any resource sharing agreements such as the Northwest Mutual Assistance Agreement (NMAA), Western Region Mutual Assistance Agreement(WRMAA), or Spare Transformer Equipment Program?

Puget Sound Energy participates in the Edison Electric Institute's Spare Transformer Equipment Program and has been since 2006.

Does the company have an incident response plan? If so, when was it most recently used or tested, and what is the timeframe for the next scheduled test?

Puget Sound Energy has a cybersecurity incident response plan – Cyber Security Incident Response Plan (CSIRP). The CSIRP was last updated on October 31, 2014 and is tested at least annually.

PSE has a physical security incident response plan for each location with PSE staff. These site specific physical security incident response plans that include designated employees for incident reponse roles were distributed to each location in Janaury 2014.

1.1.6 Risk Management

Please identify the risk assessment tools used by the company that relate to CI Security (i.e., ES-C2M2, NIST Framework, etc.).

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.

Has an independent third party reviewed the company's risk management policy? If so, who performed the review, when did it occur, and how many follow-up actions were identified

PSE has an external review of its overall cybersecurity program approximately every 12 months. Results are prioritized and added to PSE's security roadmap as appropriate. The details of the review are confidential; however, PSE would be happy discuss the details of the review during a nonpublic review session.

PSE did not have an external review of its physical risk management policy in 2014.

How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?

All activities are currently being prioritized and placed in PSE's security roadmap. Again, details can be discussed during a nonpublic review session.

PSE did not have an external review of its physical risk management policy in 2014 .

Please describe any voluntary security standards that the company has adopted.

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.

1.2 CRITICAL INFRASTRUCTURE SECURITY – CYBERSECURITY

1.2.1 Cybersecurity budget

If available, please provide the percentage of the company's entire IT budget spent on cybersecurity. If unavailable, please provide an explanation.

The cybersecurity and physical security budgets are in alignment with the security activities identified in the security roadmap.

1.2.2 Cybersecurity – Vulnerability assessments

Please provide the date of the company's most recent vulnerability assessment, who performed the assessment, and how many follow-up actions were identified.

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.). They occur on a regular basis as opposed to single points in time. All results are documented and tracked on a risk register for follow-up and remediation. The results of all security centric activities are confidential; however, PSE would be happy discuss any details during a nonpublic review session.

How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?

See above.

1.2.3 Cybersecurity – Penetration tests

Please provide the date of the company's most recent penetration test, who performed the test, and how many follow-up actions were identified.

The penetration testing program is designed to discover, validate and analyze security vulnerabilities that may reside on information technology assets. It is a component of holistic security management designed to provide coordination and oversight for various security activities performed internally on behalf of PSE. A penetration test is independently scheduled or in support of other cybersecurity activities (e.g. security assessments) to provide additional insight into valuable IT assets at PSE. The results of all security centric activities are confidential; however, PSE would be happy discuss any details during a nonpublic review session.

How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?

See above.

1.2.4 Cybersecurity – Vulnerability & Penetration (Future)

Please provide the timeframe for the company's next planned vulnerability assessment and penetration test and if the company or a third party will perform each.

Both programs for cybersecurity have been outlined above. The details behind all security centric activities are confidential; however, PSE would be happy discuss during a nonpublic review session.

1.2.5 Information-sharing and collaboration efforts

For the following information-sharing and collaboration efforts, please provide a description of the company's level of involvement with each, and complete the table below.

	Was the company involved in the effort during the calendar year?	Did the company receive alerts or information from this effort during the calendar year? If so, how often (monthly, quarterly, etc) was information from this source received and reviewed by the company?	Has the company contributed information to this effort during the calendar year?
Electricity Sector Information Sharing and Analysis Center (ES-ISAC)	Yes	Weekly industry report Ad-hoc security alerts	No
Cybersecurity Risk Information Sharing Program (CRISP)	No	No	No
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Yes	Weekly industry report Ad-hoc vulnerability alerts	No
Seattle FBI Cyber Task Force's FLASH Alerts	Yes	Quarterly cybersecurity status Ad-hoc FLASH alerts	Yes
Public, Regional Information Security Event Management (PRISEM)	Yes	PRISEM data via DHS portal	No
Cyber Incident Response Coalition for Analysis Services, (CIRCAS)	No	No	No