

Docket Nos. UE-072300 and UG-072301

**Puget Sound Energy
2016 SQ Program and Electric Service Reliability Filing**

**Attachment C:
PSE 2016 Critical Infrastructure Security Annual Report**

Puget Sound Energy
2016
Critical Infrastructure Security Annual Report

CONTENTS

| | |
|--|---|
| Critical Infrastructure Security 2016 Annual Report..... | 2 |
| 1.1 Critical Infrastructure Security – Cybersecurity and Physical Security | 2 |
| 1.1.1 Critical Infrastructure Security Policy and Teams | 2 |
| 1.1.1.1 Critical Infrastructure Security Policy..... | 2 |
| 1.1.1.2 Critical Infrastructure Security Team..... | 2 |
| 1.1.2 Critical Infrastructure Security Policy and Teams Changes..... | 3 |
| 1.1.2.1 Critical Infrastructure Security Policy Changes | 3 |
| 1.1.2.2 Critical Infrastructure Security Team Changes..... | 3 |
| 1.1.3 PSE’s External Participation | 4 |
| 1.1.4 Unauthorized actions related to cybersecurity and physical security..... | 6 |
| 1.1.5 Incident Response | 6 |
| 1.1.6 Risk Management | 7 |
| 1.2 Critical Infrastructure Security – Cybersecurity | 7 |
| 1.2.1 Cybersecurity budget..... | 7 |
| 1.2.2 Cybersecurity – Vulnerability assessments..... | 8 |
| 1.2.3 Cybersecurity – Penetration tests..... | 8 |
| 1.2.4 Cybersecurity – Vulnerability & Penetration (Future) | 8 |
| 1.2.5 Information-sharing and collaboration efforts..... | 9 |

CRITICAL INFRASTRUCTURE SECURITY 2016 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's Critical 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.

PSE has three main security related policies – a critical infrastructure cybersecurity policy, an overall physical security policy, and an overall Information Security and Acceptable Use policy.

The PSE cybersecurity policy has changed in 2016 to reflect the requirements of NERC CIP v5¹. The new policy requires PSE to develop programs, processes and procedures as required by NERC CIP v5. The programs, processes and procedures are to contain the detail necessary to address the various aspects of each NERC CIP v5 requirement.

The PSE Physical Security policy has changed in 2016 to reflect the requirements of NERC CIP v5. The new policy requires PSE to develop programs, processes and procedures as required by NERC CIP v5. The programs, processes and procedures are to contain the detail necessary to address the various aspects of each NERC CIP v5 requirement.

The overall information security and acceptable use policy has not changed in 2016.

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 change in 2016.

The roles and resources were as follow:

¹ North American Electric Reliability Corporation (NERC) critical infrastructure protection cybersecurity standards (CIP Version 5), approved by Federal Energy Regulatory Commission on November 30, 2013.

- Director/Information Security Officer (1)
- Manager, IT Security (1)
- Manager, IT Compliance (1)
- Security Architect (1)
- Advisor IT Security Analyst (4)
- Senior IT Security Analyst (6)
- IT Security Analyst (2)
- Senior Records Management Analyst (2)
- Administrative Specialist (1)

The physical security team did change in 2016.

The roles and resources were as follow:

- Manager (1)
- Senior Investigator (2)
- Physical Security Program Administrator (1)
- Security Command Center Program Manager (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.

As outlined above, there were changes made to the CI Security policy.

As outlined above, there were changes made to the Physical Security policy

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.

As outlined above, there were changes made to the cybersecurity team. Mainly, new analysts were hired in and some promotions occurred.

As outlined above, there were changes made to the Physical Security team. Mainly, the Sr. Regulatory Compliance Analyst position was dropped, and the Security Command Center Program Manager position was added.

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.

The NCC Group Assessment – In late December 2016, PSE's cyber security consulting vendor, NCC Group, conducted a security gap assessment, based on the Department of Homeland Security Cybersecurity Framework at PSE. The assessment was interview based over a two-week period. Once the interviews were complete, NCC Group provided a report to PSE outlining areas that are working well and areas that require additional attention. The results of this assessment will be utilized to build a new three year cyber security roadmap.

In early October, PSE's Information Security Officer and Chief Information Officer went to Washington DC and attended the following meetings:

- **FERC Office of Energy Infrastructure Security (OEIS)** – Meeting with FERC's OEIS to discuss new discoveries through their subsequent cyber assessments. In addition, discussed potential of engaging the OEIS for future assessments in Gas Operations, Physical Security, and Liquefied Natural Gas plant.
- **Edison Electric Institute (EEI) Cybersecurity and Reliability Team** – Meeting with EEI to discuss various initiatives they are sponsoring as well as more details behind the Electricity Subsector Coordinating Council Cybersecurity Mutual Assistance program
- **American Gas Association (AGA) Cybersecurity Team** – Meeting with the AGA to discuss various initiatives they are sponsoring.
- **David Gillers, Senior Counsel, Senate Committee on Energy & Natural Resources** – Meeting to discuss risks and opportunities in the utility cyber security arena.
- **Janet Sena, Sr. VP Public Policy, NERC** – Meeting to discuss upcoming areas of focus for NERC, how her team approaches cybersecurity policy, and PSE's implementation of NERC CIP v5.

Continuity Programs and Recovery Managers (CPARM) – PSE hosted a local CPARM event where various topics regarding business continuity and incident response were discussed. Other companies in attendance were Alaska Airlines, Amazon, and Costco.

Cyber Guard 2016 Prelude Exercise – The regional exercise involved an artificial entity that experienced an attack similar to the Ukrainian incident. The event was held at Camp Murray.

DHS Physical Security Awareness Campaign – 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 committees PSE participated in during 2016.

- Western Electricity Coordinating Council CIP User Group
- American Gas Association Security Group
- Edison Electric Institute Security Group
- Electricity Subsector Coordinating Council Cybersecurity Mutual Assistance program

- 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; or*
- iv. serious financial harm.*

PSE did not have any cybersecurity or physical security events in 2016 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?

In 2015, PSE placed on retainer or under contract outside counsel, a forensics firm, and public relations firm for support in the event of a cybersecurity incident.

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

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

Outside counsel provides general guidance and direction and assists in managing other external entities during a cybersecurity event. The forensics firm provides additional layers of expertise in managing cybersecurity attacks and tools as deemed appropriate. The public relations firm assists in communications to the public as advised by PSE and outside council.

PSE currently does not have a retainer or contract 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?

PSE has a cybersecurity incident response plan (CSIRP). The CSIRP is currently in revision with a target completion of February 28, 2017 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 response roles

were distributed to each location in January 2014. Plans were reviewed in 2016, and updates were made as required.

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 2016.

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 2016.

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 frameworks (e.g. NIST, ES C2M2). Since each process and/or framework 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 budget is 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 (We are also a member of the DNG-ISAC) | 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 | No |
| Public, Regional Information Security Event Management (PRISEM) | No | No | No |
| Cyber Incident Response Coalition for Analysis Services, (CIRCAS) | Yes | Yes Ad hoc | Yes |