PACIFIC POWER
A DIVISION OF PACIFICORP

825 NE Multnomah, Suite 2000
Portland, Oregon 97232

December 29, 2015

VIA ELECTRONIC FILING
AND OVERNIGHT DELIVERY

Steven V. King
Executive Director and Secretary
Washington Utilities and Transportation Commission
1300 S. Evergreen Park Drive SW
P.O. Box 47250
Olympia, WA 98504-7250

RE: Docket UE-140766—Pacific Power & Light Company's 2015 Critical Infrastructure Security Annual Report

Pacific Power & Light Company (Pacific Power or Company), a division of PacifiCorp, submits the following updated information on the Company's critical infrastructure (CI) and cyber security program.

The Commission's request for the Company to submit a Critical Infrastructure Security Report involves detailed information that is sensitive in nature, the release of which may create security risks to the Company, the bulk electric system and the electric network that serves our customers. PacifiCorp's responsibility to protect sensitive information requires that the Company's response be at a high level; however, the Company will provide a more detailed briefing in a private, confidential setting, if requested.

CYBERSECURITY AND PHYSICAL SECURITY

1. Critical Infrastructure Security Policy and Teams

    a. Please provide a copy of the table of contents of the Company's CI Security policy and identify any sections of the policy that have been added or modified since the last report.

    Response: No changes have been made since the Company's last report. As reference, Attachment A to this report provides the table of contents for the Berkshire Hathaway Energy Security Policies.

    b. Please provide an organizational diagram of the Company's CI Security team(s). The diagram, or accompanying list, should include the titles of staff on the team.

    Response: The Company employs a dedicated team of security professionals to manage its cybersecurity and physical security functions, but unable to share the organizational chart as it is considered security-sensitive company information.

c. 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.

Response: No changes were made to the Company's CI Security policy since the last report. Previously, the corporate information security governance for all of the Berkshire Hathaway Energy affiliates was under the direction of the PacifiCorp Vice President of IT Applications and Security. During 2015, the function was transitioned to the President of MidAmerican Energy Company, who also serves as a designated industry CEO on the Electricity Subsector Coordinating Council representing Berkshire Hathaway Energy businesses on matters of national security and resiliency. Oversight for PacifiCorp's physical security organization remained under the authority of the PacifiCorp Vice President of IT Applications and Security.

d. What internal processes does the Company use to evaluate its CI Security policy and structure?

Response: Annual review processes are in place, including consultation with a companywide policy steering group comprising senior IT leaders from each business.

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

Response: PacifiCorp participated in the NERC GridEx III exercise in November 2015.

PacifiCorp's participation in committees and conferences included:

- Electricity Subsector Coordinating Council (ESCC)
- EEI/AGA Security Committee & Conference
- CEATI – Security Infrastructure Protection Security Interest Group (IPSIG) – Chairperson

PacifiCorp receives classified briefings and attends a counter-intelligence conference.

3. Please include a list of any unauthorized actions related to cybersecurity or 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.

The list should include the following information about each event:

a. any organizations or government entities notified of the event or involved in the response to the event;
b. a description of the event and its impact;
c. whether the Company conducted a root cause analysis of the event;
d. how many follow-up actions were identified as a result of the incident;
e. how many of the follow-up actions identified in part (c.) 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; and
f. date the incident was resolved, if applicable.

Response: No incidents to report.

4. Does the Company have retainers or contracts for outside help 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? Is the Company currently participating in any resource sharing agreements such as the Northwest Mutual Assistance Agreement, Western Region Mutual Assistance Agreement, or Spare Transformer Equipment Program?

Response: PacifiCorp is eligible to participate in several commercial incident response retainers that have been negotiated at the Berkshire Hathaway Energy level. It also participates in regional and national resource sharing agreements.

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

a. Has an independent third party reviewed the Company's risk management policy?
b. If so, when did it occur, and how many follow-up actions were identified? 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?

Response: Berkshire Hathaway Energy businesses use ES-C2M2, DOE Cybersecurity Risk Management Framework and NIST Cybersecurity Framework to help them assess risks. A third-party review was conducted in 2013. Key follow-up items were completed in 2014.

6. 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?

Response: Depending on the scope and severity of an incident, an escalating set of incident response teams can be mobilized, including a corporate-level team.

The National Incident Management System (NIMS) is used as the foundation for the incident command team structures and protocols.

PacifiCorp's Cybersecurity Incident Response Plan (CSIRP) comprises information and physical security incident response strategies. The plan was reviewed through a tabletop exercise August 12, 2015. The last plan activation occurred in April 2012. The next assessment is scheduled on or about August 9, 2016.

Pacific Power and Rocky Mountain Power each have business-level incident response plans and emergency action centers in place. There is a PacifiCorp IT Emergency Action Plan and dedicated action center. The various business units are required to maintain and exercise related business continuity and technology recovery plans.

7. Please describe any voluntary security standards that the Company has adopted.

Response: Voluntary standards are leveraged to influence good security practices. PacifiCorp's cybersecurity and physical security organizations leverage the following standards when developing security practices:

- ES-C2M2
- NIST Cybersecurity Framework
- NIST 800 series
- ISO 27001
- ASIS International SPC1-2009 – Electronic Security Systems
- NFPA 730-731 – Organizational Resilience

8. Please describe any security training provided to company employees.

Response: All new hires and contractors are required to complete basic cybersecurity and physical security training. Annual CIPS refresher training is required for personnel who have access to BES assets and BES cyber assets. Beginning in 2016, annual computer-based refresher training will be required for all personnel.

A Berkshire Hathaway Energy companywide communication related to the importance of cybersecurity and diligence in maintaining a secure environment was issued in March 2015. Quarterly security awareness communications are distributed to personnel that cover topics applicable to the workplace and personal life. Ancillary communications are distributed to personnel as needed to advise them about urgent or emerging security issues or situations.

CYBERSECURITY

9. Please provide the calendar quarter of the Company's most recent vulnerability assessment. Please identify whether it was an internal or external audit, and how many follow-up actions were identified. 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?

   Response: General third-party vulnerability assessments and penetration tests are conducted every two years. The most recent assessments were conducted in 2014. Annual NERC CIPS vulnerability assessments are also conducted. The results of the assessments and status of the findings are classified as company sensitive information and may not be shared.

10. Please provide the calendar quarter of the Company's most recent penetration test. Please identify whether it was an internal or external test, and how many follow-up actions were identified. 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?

    Response: A penetration test was conducted in Q3 2014 by a third party; however, the results may not be shared. Internal penetration testing is performed on a regular basis and includes vulnerability scanning of internet-facing systems on a weekly basis.

11. 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.

    Response: A third-party vulnerability assessment will be conducted during 2016, but the date has not yet been scheduled.

12. 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.

    Response: Many sources are leveraged to measure the effectiveness of the Company's security controls. Collaboration with the industry and public/private stakeholder groups is promoted. The focus is on advancing program maturity and threat identification and mitigation. The Company also engages in a variety of classified information sharing programs and several key security and executive team personnel hold a government-sponsored clearance. The specific classified information sharing engagements is considered sensitive and can be shared verbally with the Commission and staff in a closed meeting.

	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 (E-ISAC)	Yes	Yes – Weekly	No
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Yes	Yes – Daily, Weekly	No
Seattle FBI Cyber Task Force's FLASH Alerts	Yes	Yes – When issued	No

Please direct any informal inquiries regarding this filing to Ariel Son, Regulatory Projects Manager, at (503) 813-5410.

Sincerely,

R. Bryce Dalley
Vice President, Regulation

cc: Jason Ball, WUTC Staff

Attachment A: Berkshire Hathaway Energy Information Security Policies

TABLE OF CONTENTS