

September 19, 2014

***VIA ELECTRONIC FILING  
AND OVERNIGHT DELIVERY***

Washington Utilities and Transportation Commission  
1300 S. Evergreen Park Drive SW  
P.O. Box 47250  
Olympia, WA 98504-7250

Attn: Steven V. King  
Executive Director and Secretary

**RE: Critical Infrastructure Security Annual Report  
Docket UE-140766 – Pacific Power & Light Company’s Annual Service Quality  
Report for 2013**

Dear Mr. King:

Pacific Power & Light Company, a division of PacifiCorp (PacifiCorp or Company) provides the following response as the Critical Infrastructure Report requested by the Washington Utility and Transportation Commission (Commission) Critical Infrastructure Security Team (Team) via email on July 29, 2014. The Company looks forward to participating in the meeting scheduled by the Team for October 22, 2014, to address any questions regarding the reports in this docket.

The Commission’s request for PacifiCorp 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 our response be at a high level; however, the Company looks forward to providing a more detailed briefing in a private, confidential setting.

**CORPORATE SECURITY AND RISK ORGANIZATION**

The cybersecurity and physical security functions at PacifiCorp are centralized under the Corporate Security and Risk organization. PacifiCorp’s philosophy is to ensure prudent application of appropriate risk management techniques to minimize the likelihood or impact of risks that could significantly affect the Company’s personnel, property or ability to perform critical operations that serve customers and stakeholders.

The Company’s security program focuses on development and implementation of strategic, global security policies and practices. The organization is responsible for enterprise-wide security monitoring and alerting, including event analysis and incident response. The program promotes consistency in the application of policies and practices; provides forums to discuss

security incidents, issues, threats and emerging trends; facilitates an annual review of security policies and standards; and ensures development of standards, procedures, controls and guidelines that support a stable and secure operating environment.

### **VOLUNTARY AND MANDATORY STANDARDS**

PacifiCorp leverages a wide variety of voluntary standards to aid in the design and application of good security practices, example sources include U.S. Department of Homeland Security, U.S. Department of Energy, ASIS International, International Organization for Standardization (ISO), National Institute of Standards and Technology's (NIST) Standard Reference Materials and Cybersecurity Framework, and Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The Company also complies with mandatory standards, including North American Electric Reliability Corporation (NERC) Reliability Standards and Critical Infrastructure Protection Standards (CIPS).

### **INFORMATION SHARING AND COLLABORATION**

Although traditional protective security controls are important, they are not sufficient to protect against all vulnerabilities and emerging threats. PacifiCorp engages with many information sharing and threat awareness sources to aid in measuring the effectiveness of its security controls and to collaborate with industry peers and national, state and local agencies to address common security issues.

PacifiCorp places significant emphasis on adaptive security measures related to identification of new and emerging threats. The Corporate Security and Risk Organization actively monitors physical and cybersecurity alerts and advisories from a variety of sources, including U.S. Department of Homeland Security US-CERT, ICS-CERT and Homeland Security Information Network (HSIN), Electricity Sector Information Sharing and Analysis Center (ES-ISAC), state fusion centers, industry groups, peer organizations, local and regional agency contacts, and security vendor resources. The information gleaned from these sources aids in the Company's awareness, evaluation and application of mitigation measures.

### **ASSESSMENTS AND TESTING**

PacifiCorp supports a variety of strategies to assess its security posture. In cooperation with the internal audit organization, third-party vulnerability assessments and penetration tests are conducted every other year. Different third parties are used to provide variation in the processes, tools and skills that are applied to assess the Company's security. The final assessment reports are submitted to the executive team and key stakeholders. The Company also participates in federal, state and industry assessment programs, ensures assessments required to comply with

regulatory and other standards are completed (e.g., NERC CIPS and EOP), and conducts additional internal assessments to evaluate its security measures and controls.

### **INCIDENT RESPONSE AND EXERCISES**

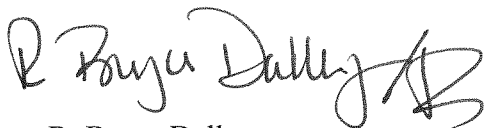
PacifiCorp has a strong culture of incident response and management practices. Incident response, cybersecurity incident response, business continuity and technology recovery plans are in place and exercised at a minimum annually. Depending on the scope and severity of an incident, an escalating set of incident command teams can be mobilized for response, including a Company-level incident command team. The National Incident Management System (NIMS) is used as the foundation for incident command team structures and protocols. Cybersecurity, business continuity and technology recovery plans may be activated to support incident command team objectives. Third party agreements are in place to facilitate requests for assistance when additional resources, skill sets and assets may be needed to respond to or recover from an event.

A wide spectrum of tabletop and functional exercises are conducted to evaluate the strategies in PacifiCorp's plans. Local and regional law enforcement and response agencies are often invited to participate in the exercises, and the Company periodically participates in exercises conducted by local, regional and national entities.

Comprehensive reviews are conducted after key exercises and incidents to identify and document lessons learned. The information is shared with response team members and organizational stakeholders and used to improve the Company's plans and programs.

Please direct any informal inquiries regarding this filing to Natasha Siores, Director, Regulatory Affairs and Revenue Requirement Affairs, at (503) 813-6583.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Bryce Dalley" with a stylized flourish at the end.

R. Bryce Dalley  
Vice President, Regulation

cc: Jason Ball, WUTC Staff