e-FILING REPORT COVER SHEET

REPORT NAME: PacifiCorp's Response to Cybersecurity Workshop Questions

COMPANY NAME: Pacific Power

DOES REPORT CONTAIN CONFIDENTIAL INFORMATION? ☒ No ☐ Yes
If yes, please submit only the cover letter electronically. Submit confidential information as directed OAR 860-001-0070 or the terms of an applicable protective order.

If known, please select designation: ☒ RE (Electric) ☐ RG (Gas) ☐ RW (Water) ☐ RO (Other)

Report is required by:
☐ OAR
☐ Statute
☐ Order
☒ Other At request of Commissioners at Dec 6, 2011 Workshop

Is this report associated with a specific docket/case? ☒ No ☐ Yes
If Yes, enter docket number: UM 1484

Key words: cybersecurity

If known, please select the PUC Section to which the report should be directed:

☐ Corporate Analysis and Water Regulation
☐ Economic and Policy Analysis
☐ Electric and Natural Gas Revenue Requirements
☐ Electric Rates and Planning
☐ Natural Gas Rates and Planning
☒ Utility Safety, Reliability & Security
☐ Administrative Hearings Division
☐ Consumer Services Section

PLEASE NOTE: Do NOT use this form or e-filing with the PUC Filing Center for:

- **Annual Fee Statement form and payment remittance or**
- **OUS or RSPF Surcharge form or surcharge remittance or**
- **Any other Telecommunications Reporting or**
- **Any daily safety or safety incident reports or**
- **Accident reports required by ORS 654.715.**

PACIFICORP
A MIDAMERICAN ENERGY HOLDINGS COMPANY

PacifiCorp's Response to Cybersecurity Workshop Questions

At the Public Utility Commission of Oregon (Commission) Cybersecurity Workshop on December 6, 2011, the Commission asked the participating utilities to provide answers to questions posed in the *Cybersecurity Landscape for the Utility Industry and Considerations for State Regulators* presentation provided by EnergySec. PacifiCorp submits the following responses.

1. ***Who is ultimately responsible for cybersecurity in your organization?***

   Michael Ball, Director of Corporate Security.

2. ***How many dedicated security staff do you have?***

   The security operations team consists of eight staff members, including one manager.

3. ***What security training/ education/ awareness are you providing to all staff and how often?***

   All permanent and contract personnel are included in the scope of PacifiCorp's Security Awareness and Training Program. The core of the program consists of annual training required for all personnel as well as quarterly security awareness communications. The annual security awareness training consists of a computer-based module that was developed in house. The module covers security topics such as passwords, malware, social engineering, portable devices, physical security and sabotage reporting. The quarterly security awareness communications cover both cyber and physical security topics applicable both in the workplace and personal life. Attachment 1 provides copies of recent quarterly communications. These efforts are supplemented on an as-needed basis with additional ancillary communications used for urgent or emerging security issues. Attachment 2 is an example of supplemental material that is available on the Company's internet portal.

4. ***Are you participating in local, state, regional, national security/ disaster or energy assurance exercises?***

   Yes. In addition to a rigorous program of internal exercises, PacifiCorp regularly engages in exercises with local, state, regional and national entities for security, disaster and energy assurance exercises. Examples include:

   - Utah ShakeOut Logistics (May)
   - ESF 12 Energy Sector Cyber Attack (August)
   - Oregon Emergency Management and FEMA Region 10, Cascadia Seismic and Tsunami Impacts (August)
   - Oregon Emergency Management Association (OEMA) conference (October)
   - Portland Local Energy Assurance Planning (LEAP) Table Top Exercise (November)
   - Western Regional Mutual Assistance Agreement Partners (November)
   - Bonneville Power TIMPEX 12 Exercise (December)

5. ***Are you using the DHS/ MS-ISAC Procurement Language or IEC 62443?***

Security-related language is included in our procurement processes and resulting agreements. Rather than rely on a single standard as a basis for procurement language, PacifiCorp draws from a variety of standards and recognized good practices that focus on security. With many different types of agreements, language will vary widely based on the type of agreement for equipment, supplies or services.

An example is a security requirement for a third party service that hosts competitive bids for PacifiCorp. The security controls were evaluated in the request for proposal process and was a factor in the selection criteria. In addition, the resulting agreement included requirements to provide PacifiCorp on an annual basis, results of an annual security audit that is conducted by an independent auditing firm. In this example, security controls are included in the requirements used for the search and selection of a service provider and is also included in the resulting agreement to ensure that strong security controls remain in place.

6. ***Where do you get your situational awareness data?***

Situational awareness is obtained from a wide variety of resources that are monitored on a daily basis. Key examples include:

- U.S. Department of Homeland Security
  - Homeland Security Information Network (HSIN)
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - United States Computer Emergency Readiness Team (US-CERT)
  - Daily Open Source Infrastructure Report
- U.S. Dept. of Energy Office of Electricity Delivery and Energy Reliability (Energy Assurance Daily)
- Federal Emergency Management Agency National Situation Update
- North American Electric Reliability Corporation alerts
- Energy Central eNews
- Industry sources – EnergySec
- Antivirus and security vendors – Symantec, McAfee
- Security web sites
  - DataLoss (http://datalossdb.org)
  - Internet Storm Center (http://isc.sans.org/)
  - SearchSecurity (http://searchsecurity.techtarget.com/)
  - Arbor Networks Atlas Initiative (http://atlas.arbor.net)

7. ***What cybersecurity technologies do you use (general platforms, not specific technologies)?***

PacifiCorp uses a wide variety of cybersecurity technologies, including:

- Antivirus and anti-malware on corporate servers and workstations
- Firewalls and firewall security assessment and server profiling solutions
- Virtual private network (VPN)
- Multi-factor authentication systems
- Centralized Security Information and Event Management (SIEM)
- Application source code security scanning
- Application and network penetration testing solutions
- Wireless and modem security scanning

8. ***How frequently do you perform an exhaustive inventory of all control systems and associated communication links?***

   Annually.

9. ***Can the ICS networks be intelligently islanded from corporate networks and the Internet?***

   Yes, and as a basic security control network, it should be isolated. Network isolation and separation continues to be the greatest single security control that reduces risk to these systems. Communications crossing the boundary of an ICS network are subject to strict controls and monitoring.

In addition to providing answers to the questions cited in the EnergySec presentation, the Commission asked how they may best engage the utilities related to cybersecurity.

PacifiCorp suggests the most valuable ways to participate are to remain aware of cybersecurity issues and seek to understand how the utilities manage and adapt to evolving threats. The December 6, 2011, cybersecurity workshop was a good example of such an activity. PacifiCorp would be happy to provide an annual update to the Commissioners of its cybersecurity program. Additionally, since 2007, the Company has had meetings with Commission Staff to discuss the company's views on reliability standards and cybersecurity issues. The Company is available to meet with Commission Staff on a more regular basis if that would be beneficial to the Commission and its staff.

Attachment 1

From: PacifiCorp Security
Sent: Monday, February 28, 2011 9:41 AM
To: _ALL Emp excl BCC & EW
Subject: Critical Infrastructure Protection Standards regulatory requirements

COMPANY CONFIDENTIAL INFORMATION – FOR INTERNAL USE ONLY

Supervisors, please share this information with employees who do not have access to e-mail.

A message from Michael Ball, director, corporate information security

WHAT IS HAPPENING AND WHY?

In compliance with the North American Electric Reliability Corporation, PacifiCorp regularly provides employees with information about its Critical Infrastructure Protection Standards. This message is to reinforce company and regulatory requirements for the transmission of information related to PacifiCorp's critical infrastructure (facilities or cyber assets), also known as "Critical Infrastructure Information" or "CII".

CII is information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII is considered information concerning proposed or existing critical assets and the associated critical cyber assets related to the production, generation or transmission of energy.

WHAT DO I NEED TO DO?

All documentation containing critical CII must be transmitted in an appropriate manner according to the following guidelines:

- Internal transmission of CII
  - CII may be transmitted within PacifiCorp in hard or softcopy form using corporate e-mail, interoffice mail or portable media devices.
  - Reference to CII must be noted in the subject line of e-mails containing CII and the following disclaimer must be included in the body of the e-mail.

    Disclaimer: The sensitivity of the information contained in this e-mail has been classified under the PacifiCorp Data Classification Program as CII. The recipient of this information is required to follow the procedures outlined in the PacifiCorp Critical Infrastructure Information Procedure.

  - Reference to CII must be noted on interoffice mail envelopes when CII is included.
  - CII transmitted using portable media devices must be protected at all times.
- External transmission of CII
  - Hard copies of CII or soft copies stored on portable media devices may be transmitted in the possession of PacifiCorp personnel or by U.S. first class, express, certified or registered mail or other bonded courier.
  - Electronic CII must be encrypted before transmission.
  - CII may be transmitted through e-mail using encrypted files, such as WinZip with a strong password.
    - Reference to CII must be noted in the subject line of the e-mail.
    - The password must not be included in the transmittal e-mail. It should be provided by telephone or through an unrelated e-mail not mentioning the document name.
    - Password-protected Microsoft Office documents do not meet encryption requirements.
  - Secured file transfers to external (Internet) sites or internal (intranet) sites must be sent to a specific IP address and be protected by a password. Contact the Enterprise Service Desk via e-mail or call 503-813-5555 or 801-220-5555 for assistance with such transfers.

You can find information regarding the CII procedure, including instructions for identifying, handling and declassifying CII, as well as

other material related to CIPS, at the following intranet page: http://idoc.pacificorp.us/e-resources/nc/ncppf.html. Please review this information and refresh your familiarity with the policies and procedures as some of the content such as instructions for declassifying CII are new.

Thanks for your cooperation in keeping PacifiCorp's critical information secure and helping ensure the company is in compliance with NERC requirements.

Michael Ball
Director, corporate information security

From: PacifiCorp Security
Sent: Tuesday, May 24, 2011 10:14 AM
To: _ALL Emp PCORP & MNG
Subject: Be alert for phishing attempts

COMPANY CONFIDENTIAL INFORMATION – FOR INTERNAL USE ONLY

Supervisors, please share this information with employees and contractors who do not have access to email.

A message from Michael Ball, director, corporate security

Be alert for phishing attempts

Epsilon, a major email marketing services company used by retailers such as Best Buy, Kroger and Target and credit card companies like JPMorgan Chase, Citi, Barclays and Capital One, recently reported its database was hacked and the names and email addresses of approximately 2 percent of its client's data was compromised. While no personal financial information was disclosed, the company issued a warning that affected customers were at risk of increased spam and potential phishing campaigns.

Phishing is an attempt directed at an individual, usually via email, to insert spyware on a computer or acquire confidential information, such as a username, password, Social Security Number, bank account or credit card data. The phisher pretends to be a company you may have done business with in the past, a bank or some other legitimate and trustworthy organization.

Avoid phishing attacks

- **Be cautious**
  - Do not open email or attachments from unknown sources.
  - Be suspicious of email with urgent requests for personal information.
  - Look for spelling errors in email addresses, URLs or in the body of a message. Be especially wary of URLs that do not end in ".com".
  - Never enter personal information in a popup window or on an unknown website.
  - Navigate to the company's website by entering the known URL in the address bar of your browser, do a search for the company's contact information, or check the last bill received from the entity to validate the company's contact information, including customer service telephone numbers.
  - Use the information from your search to contact the company to confirm the validity of the request. Never use phone numbers or email links contained in an email.
  - Legitimate companies have access to customer log-in and password information and will not solicit customer calls to confirm the information or validate information on a website.
  - Always use shift + delete to remove the message from your email account.

- **Be proactive**
  - Make sure you are using a secure website when submitting financial and confidential personal information.
  - Change your passwords frequently.
  - Use strong passwords that include upper and lowercase letters, numbers and special characters.
  - Don't use the same password on multiple sites.
  - Regularly log into online accounts to monitor activity and check statements.
  - Use anti-virus, anti-spam and firewall software to protect your computer.
  - Keep your operating system and applications up-to-date

Take action

If you receive an email that may be a phishing attempt, forward it to spam@uce.gov and to the company that was impersonated. Most organizations have information on their websites about where to report problems. The company's information security department may want you to forward the message to them for further investigation.

If you believe you were the victim of a phishing scam, report it to the Federal Trade Commission at www.ftc.gov/complaint.

For additional information visit the Anti-Phishing Work Group website at www.antiphishing.org.

From: Compliance
Sent: Monday, August 08, 2011 8:59 AM
To: _ALL Emp PCORP & MNG
Subject: Sabotage reporting and critical infrastructure information

COMPANY CONFIDENTIAL INFORMATION – FOR INTERNAL USE ONLY

Supervisors, please post this bulletin in a noticeable location and share it with all employees, contractors and vendors in your organization who do not have access to email.

A message from Michael Ball, director, corporate security

Sabotage Reporting

PacifiCorp is required to report suspected or actual disturbances or unusual occurrences associated with sabotage to the appropriate governmental agencies and regulatory bodies including law enforcement.

Sabotage is a deliberate behavior intended to cause disruption in a work or social environment. It often involves destruction of property or obstruction of normal operations, but it also may include unauthorized or suspicious physical, photographic or electronic surveillance at a business site. Sabotage attempts may be related to terrorism or disruptive workplace events.

Sabotage of the bulk electric system may include:

- Tampering with transmission towers or poles.
- Disrupting the supply of fuel to a generation plant.
- Disrupting business operations through false or real threats (e.g., bomb, fire, tampering).
- Causing intentional failure of critical equipment or systems.
- Deliberately cutting fiber optic lines supporting control systems or other essential communications.
- Successful cyber intrusion into a control system.

Sabotage awareness and reporting is essential to protect the bulk electric system and the interests of PacifiCorp, its customers and key stakeholders. Procedures to complete the required documentation and reporting are in place; however, the first step is awareness of situations that may represent a threat or result in sabotage. It is important that personnel be attentive to, recognize and report known or suspected acts of sabotage to initiate appropriate response activities.

To report known or suspected sabotage:

- Contact 911 if the situation requires an immediate response.
- Call the Technology Resource Center (503-813-5555) and press "1" for an emergency when prompted.
- Complete a Security Incident Reporting Form, which can be accessed at http://securityincident.pacificorp.com/securityreport/index.jsp

---

Reminder: Critical Infrastructure Information

Critical infrastructure information is not customarily in the public domain. The information is related to the security of critical infrastructure or protected systems. It is a FERC requirement that this information be protected, in both electronic and printed formats, at all times. Please remember to place a disclaimer in all emails containing CII. A sample disclaimer statement is provided below:

> ***Disclaimer: The sensitivity of the information contained in this email has been classified under the PacifiCorp Infrastructure Information Program as Critical Infrastructure Information. The recipient of this information is required to manage the information as outlined in the PacifiCorp Critical Infrastructure Information Procedure.***

Critical infrastructure information program and procedure document may be accessed at: http://idoc.pacificorp.us/e-resources/nc/oc/cr.html

From: PacifiCorp Security
Sent: Tuesday, December 20, 2011 9:04 AM
To: _ALL Emp PCORP & MNG; _ALL Contractors
Subject: Q4 2011 Security Awareness Bulletin: Facility Access and Identification

SUPERVISORS, PLEASE SHARE THIS INFORMATION WITH PERSONNEL WHO DO NOT HAVE ACCESS TO EMAIL. BULLETIN BOARD ADMINISTRATORS, PLEASE POST THIS MESSAGE ON COMPANY BULLETIN BOARDS.

A message from Michael Ball, director, corporate security

The safety and security of personnel and visitors at PacifiCorp is of the utmost importance. This is why it is very important to review and refresh our knowledge of the policies and procedures each of us are responsible for following to ensure we maintain a safe and secure work environment. Please take a few minutes to review our basic security expectations.

Access to Secured Areas
You are required to swipe your company-issued identification badge prior to entering a secured area, even if your badge was not used to open the door. Be watchful of individuals who may attempt to enter the area after you without swiping a badge. This is called "tailgating", and it is strictly prohibited. If an individual does not possess a badge, direct or escort the person to site security, if available, or contact an on-duty supervisor. **DO NOT** allow anyone to enter a secured area without proper authorization.

Identification Badges
Personnel must visibly display company identification badges at all times. Certain technical or craft personnel may be authorized by management to temporarily remove their badge if it creates a hazard or may be lost or damaged by work activities; however, these exceptions should be kept to a minimum.

Only one authorized identification badge may be issued to an employee, contractor or vendor at a time. At some facilities, an individual whose badge is temporarily unavailable, but not lost or stolen, may obtain a temporary badge from the site security desk, badge office or designated badge issuer for the facility. The individual must present a valid photo ID and only will receive a temporary badge if they already are authorized for unescorted access in secured areas.

Lost or stolen badges must be reported to security immediately. Access privileges associated with the lost or stolen badge will be suspended until the badge is recovered or reissued. At some sites, temporary access badges may be available during normal work hours. Personnel may obtain replacement badges from a badging office during its normal hours of operation. Replacement badges may be issued outside of the office's business hours on an emergency basis by contacting corporate security at 503-813-6481 in Portland or 801-220-2224 in Salt Lake City.

All personnel must return their company-issued identification badge to their manager or supervisor when ending their affiliation with PacifiCorp. In most cases, it is the manager or supervisor's responsibility to collect the badge at termination and return it to the issuing authority. Retention of a badge after employment ends could enable an unauthorized individual to falsely represent PacifiCorp, and in some cases disrupt business operations.

Visitors
Visitors always must be escorted while in secured areas. Follow all access control and logging procedures at your facility, such as signing visitors in and out, and modified after-hours procedures. Visitors should not be escorted into secured areas to wait for the person they are visiting. Safety guidelines and related information should be shared with all visitors who are on-site for more than an incidental meeting. The guidelines are posted in all conference rooms at PacifiCorp's corporate offices and are available on the intranet at http://idoc.pacificorp.us/safety_and_occupational_health/cohs/vsg.html. These guidelines also apply to personnel from other company facilities who do not regularly work at the site. A Visitor Safety Guidelines Checklist is available to assist you with this process.

Security Violations and Discipline
Get to know the individuals in your work area. Be aware of strange or unusual situations and people you don't recognize or who are acting suspiciously. If you observe a suspicious individual or situation, immediately report it to your manager or

supervisor, who will follow the appropriate operational procedures. If the individual or situation appears to present a direct physical threat, contact site security and/or 9-1-1 and avoid the threat to the extent possible.

Individuals who violate corporate security policies will be subject to PacifiCorp's disciplinary policies.

Questions
Thank you for diligently following these important procedures. If you have questions about these expectations, email Corporate Physical Security. If you need to report a security incident, call 503-813-5555 or 801-220-5555.

Attachment 2

Cyber Security: Understanding Malware

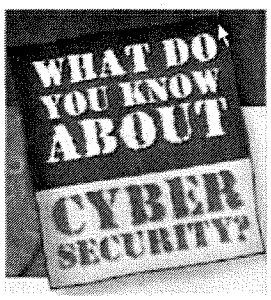
Even with top-notch antivirus software and proper precautions, malicious malware can enter a computer system. Understanding the type of attack can help users find a solution when researching or describing the problem to the Enterprise Service Desk.

The most common types of malware include:

- **Virus:** A self-replicating program designed to cause damage or mischief that inserts itself into a software program on a computer. Viruses spread from computer to computer, most often through infected e-mail or Web sites.
- **Worm:** Self-contained program similar to a virus that spreads via networks and does not need to become part of another program in order to spread. Worms infect an operating system and act like a program.
- **Trojan Horse:** A malicious program that may appear harmless – or even useful – but can conceal and download other malware that compromises the security and function of a computer.
- **Spyware and Adware:** Spyware is a malicious program that secretly installs itself on a computer and monitors and reports online activity and personal information to third parties. Adware is a kind of spyware that generates pop-up ads.
- **Keyloggers:** Spyware that secretly monitors keystrokes and sends the information to a third party.

If you suspect your computer has been infected by any of these types of malware, call the Enterprise Service Desk immediately at 503-813-5555 or 801-220-5555.

Take it home – What Can You Do If Your Computer Is Infected?



Employee Communications Archive

What we detect

Who creates malware and why?

Have you ever wondered who creates malware? Or why they do it? Find out more about the people behind the threat - the script kiddies, virus writers, and cybercriminals – and what motivates them.

Classification

Trojans, viruses, worms, dialers – the programs we detect have lots of different names. Find out how Kaspersky Lab and other antivirus companies classify the many different types of programs which can harm your computer or your data.

History of Malicious Programs

Do you know the name of the first computer virus? Or perhaps you want to find out when the first email worm was created. This section covers the evolution of malicious programs from their initial appearance to the present day.

What if my computer is infected?

With the number of threats rising every day, you may find that your computer has been infected. Find out more about the symptoms of infection, and what steps you should take to clean your computer.

Analysis

Dec 12 2011

Monthly Malware Statistics: November 2011

The following statistics were compiled in November using data collected from computers running Kaspersky Lab products

Dec 01 2011

Legit bootkits

Various proactive antivirus protection tools are capable of hooking system functions in one way or another. Malicious code also uses algorithms of this type.

Nov 16 2011

IT Threat Evolution: Q3 2011

A simple message on a Google forum in August sparked an investigation which would eventually bring down the DigiNotar certificate authority.

Nov 07 2011

Monthly Malware Statistics: October 2011

The following statistics were compiled in October using data collected from computers running Kaspersky Lab products: 161,003,697 network attacks were blocked.

Oct 13 2011

Monthly Malware Statistics: September 2011

The following statistics were compiled in September using data collected from computers running Kaspersky Lab products

Oct 06 2011

ZeuS-in-the-Mobile – Facts and Theories

Online banking is now a run-of-the-mill affair for most.

Weblog

14 Dec, 13:10 GMT
Kurt Baumgartner »
Events | Patch Tuesday December 2011

13 Dec, 09:48 GMT
Vyacheslav Zakorzhevsky »
Research | New Exploit Targeting Java Vulnerability Found in BlackHole Arsenal

08 Dec, 09:04 GMT
Ryan Naraine »
Webcasts | Lab Matters - Java exploits percolate

07 Dec, 08:31 GMT
David »
Project | Malware Calendar Wallpaper for December 2011

06 Dec, 18:21 GMT
Fabio Assolini »
Virus Watch | Malicious Boot loaders

01 Dec, 08:30 GMT
Ryan Naraine »
Webcasts | Lab Matters - Analyzing the Android security ecosystem

30 Nov, 15:10 GMT
VitalyK »
Incidents | The Mystery of Duqu: Part Six (The Command and Control servers)

securelist.com
Threats
Analysis
Blog
Descriptions
Glossary
RSS feeds
Contacts
Search

kaspersky.com
Products
eStore
Threats
Downloads
Support
Partners
About Us
Search