DOCKETED	
Docket Number:	23-SB-02
Project Title:	SB X1-2 Implementation
TN #:	250704
Document Title:	WSPA SBX1-2 Security Question Responses
Description:	CEC responses to WSPA's data security questions
Filer:	Andrea Baley
Organization:	California Energy Commission
Submitter Role:	Commission Staff
Submission Date:	6/21/2023 3:44:54 PM
Docketed Date:	6/21/2023

The Western States Petroleum Association (WSPA) submitted comments on 5/30/2023 to docket 23-SB-02 containing questions on how the California Energy Commission (CEC) protects sensitive data. Those questions are listed below with CEC responses. As a matter of information security, the CEC cannot publicly discuss details of our security policies, safeguards, or infrastructure that could aid a malicious actor in attempting to compromise those systems. For this reason, many of the responses below are intentionally less detailed than the question requests. The CEC has attempted to provide as complete a response as possible in a public venue. All CEC responses are in **bold**.

CEC responses to bulleted questions from pages 13-14 of the WSPA comments.

- Will CEC have a notification process for regulated entities who do not submit complete data and, if so, what form will that process take? A grace period should be factored into such a process to allow for compliance.
  Submissions will be manually reviewed by CEC staff, who will notify submitters of any issues. This process will be very similar to outreach regarding other data submissions under the Petroleum Industry Information Reporting Act (PIIRA).

- Is the CEC confident, and how so, in the capabilities of its IT system to handle the market sensitive data and other reporting data to be collected under SBX1-2?
  The CEC has successfully collected and managed data under earlier PIIRA collection efforts without incident, and we are confident in our ability to continue doing so.

- How will the CEC ensure confidentiality of the sensitive data provided to the Commission under SBX1-2?
  This question is too broad to provide a comprehensive answer. However, high-level measures the CEC takes to ensure confidentiality include, but are not limited to, the following:
  - **The CEC complies with all standards and regulations required by the California Department of Technology (CDT), including the State Information Management Manual (SIMM) and State Administrative Manual (SAM), which are largely based on National Institute of Standards and Technology (NIST) standards.**
  - **All CEC staff accounts require complex passwords and Multi-Factor Authentication (MFA) to be enabled and used to access CEC data.**
  - **All CEC staff are required to take annual cybersecurity & awareness training.**
  - **All CEC staff who work with confidential data are required to take confidentiality and data handling training.**
  - **All CEC devices have encrypted hard drives as well as other software-based security requirements (e.g. inactivity logoff, password required after sleep, etc.) to ensure only authorized users can access the device.**
  - **All CEC devices are protected from attack via an Enterprise security solution, which includes virus, malware, and advanced threat protection.**
  - **The CEC utilizes a secure Virtual Private Network (VPN) solution.**
  - **A centralized Security Operations Center (SOC) monitors Security Information and Event Management System (SIEM) logs.**

- What steps will CEC take to identify and mitigate any breach of security?
  The CEC is monitored by the California Natural Resource Agency's (CNRA) SOC, which has access to all server logs, workstation logs, and network logs including firewall which employs an intrusion prevention system (IPS).

- Would the CEC be willing to engage a third party to monitor and ensure stringent IT security measures to protect data reported?
  The CEC is already subject to regular third-party policy and security audits, which include physical examination of CEC systems and penetration testing.

CEC responses to numbered questions from Attachment B (pages 16-17) of the WSPA comments.

1. Has an information security governance framework been established, maintained and monitored? Which industry standard information security framework is this based on (e.g., ISO/IEC, NIST, CIS)?

The CEC follows standards and regulations required by the California Department of Technology (CDT), which are based on National Institute of Standards and Technology (NIST) standards and subject to audits that ensure our compliance.

2. Is a review or audit of framework controls performed regularly? Please provide an example audit report (a redacted report is acceptable).

The CEC is subject to regular third-party policy and security audits, which include physical examination of CEC systems and penetration testing. The CEC does not have a redacted report available for public review.

3. Is a rigorous information risk analysis undertaken for each critical information system? Which industry standard risk analysis framework is this based on (e.g., ISO/IEC, NIST, CIS)?

Any new systems undergo a risk assessment as prescribed by CDT. If a system meets specified requirements, a full impact assessment is performed as well.

4. Is an information security review or audit of all third-party service providers performed? Please describe the process.

Third-party access to sensitive CEC data or systems is reviewed, depending on the nature of the third party and access required, by staff within the CEC's Chief Counsel Office, Information Technology Services Branch, and the office of our Information Security Officer. These reviews may include the production of security certifications, attestations and nondisclosure agreements, and review of the party's Information Security Program.

5. Have third party penetration tests been performed? Please provide an executive summary or report of the results (a redacted report is acceptable).

See question 2.

6. Are key information security performance indicators (such as patch status, results of risk assessments, internal audits, and incident documentation) or metrics reported on a regular (e.g. monthly) basis? Please provide sample information security management status report (a redacted report is acceptable).

This information is provided to relevant managers via report dashboards generated by endpoint management software.

7. How long does the CEC intend to keep the data provided? Will all provided data be purged when it is no longer needed, and will companies be notified when it has been removed or shared beyond the scope of the law requirements?

The CEC has not yet established a retention timeline for this data. When a timeline is established, data will be deleted as it reaches the retention threshold. The CEC does not notify submitters when data has been removed or used unless required by applicable law or regulation.

8. Are systems and networks which host the repository monitored continuously and IDS/IPS systems employed to detect/prevent security events?

The CEC firewall within CNRA's network employs an IPS which feeds logs to their SOC.

9. Do you have a Security Operations Center or alert on-call staff 24/7?

Yes. CEC systems are monitored by the CNRA SOC, which has all our logs forwarded to their SIEM.

10. Is an approved method for identifying, maintaining, and protecting Personally Identifiable Information (PII) applied to ensure that information about individuals is used in compliance with legal and regulatory requirements for information privacy?

CEC use of PII is governed by State law. It isn't clear what this question means by an "approved method", but the CEC adheres to requirements for handling and protecting PII.

11. What methods(s) are used to transfer data into the repository? (e.g., API, FTP, other?)

Data collection for SB X1-2, along with the rest of PIIRA data, will utilize the CEC's Data Submission Portal (DSP). The DSP is a secure website built to receive electronic data submitted to the CEC. The DSP is built in Amazon Web Services (AWS) and utilizes AWS services to secure the data in transit and at rest. This is also true for data that is moved to the data warehouse or our on-premise network.

12. Is all data encrypted both at rest and in transit? What encryption algorithms will be used? Who will generate and hold the encryption keys?

Yes, data is encrypted in transit and at rest. The rest of this question is too sensitive for a detailed response.

13. What restrictions will be in place to prevent downloading or copying of data to unauthorized devices and users? Will users be able to access the information using mobile devices?

Access to confidential data is restricted to only authorized personnel and CEC-approved devices. The CEC achieves this through a combination of physical and policy restrictions.

14. Are backups of the repository taken (or is it replicated to another repository)? Where are they stored and how are they protected?

Data stored on our on-premise network are backed up within the CNRA data center. Data stored in cloud services is backed up, and secured, within those managed services.

15. Describe the breach notification process? Would notifications to customers in the event of a breach be within 24 hours or less?

CEC has specified agreed response times when an event is noticed and sent by CDT SOC to us for a confirmation or false positive response. We also will receive alerts from the CNRA SOC if anything suspicious shows up in which they require a similar response.

16. Is there a patch management process in place? Please provide patching timelines for 0-day, critical, high, and medium vulnerabilities.

Patch management is in place for CEC devices. All servers are patched regularly, and workstation patching occurs as needed. The CNRA SOC advises tenants on critical issues as identified by vendors and the federal government.

17. Do the administrators of the repository have malware prevention process in place (e.g. antivirus)? What is the timeline for definition updates?

Yes, CEC utilizes a malware and antivirus solution on all CEC workstations, which are updated regularly.

18. Are wireless networks secured according to an industry best practice including segmentation of guest and corporate wireless networks and encryption?

Yes.

19. Is multi-factor authentication required for all users who will have access to the data (including cloud administrators)? Is just-in-time privilege elevation enforced for cloud administrators? What authentication protocols are used?

The external network access is protected using MFA. Additional protections are in place to govern internal network access and role based permissioning. The rest of this question is too sensitive for a detailed response.

20. Are all user activities continuously logged, monitored, and reviewed on a regular basis? Are logs aggregated into a centralized Security information and event management, (SIEM)?

The centralized CNRA SOC reviews SIEM events on all CEC devices.

21. Are secure coding best practices employed by the developers of the portal/repository? What best practice standards are used? Are static and dynamic code tests performed on the portal/repository?

Yes. Our application development team conducts both static and dynamic code reviews and utilizes Veracode.

22. Describe in detail how each company's data is separated from other companies' data. Will separate encryption keys be used for each company's repository?

The CEC does not wish to publicly discuss the details of internal data organization or encryption.

23. Describe your access control policies and procedures in detail (both for reading and writing to the repository) Is access restricted to authorized locations and users? If so, how often is the access reviewed?

The data is restricted to authorized users, utilizing a least privileges model and role-based access controls, with only network staff having full access to all logs monitored by the SOC.

24. Describe in detail what controls are in place to prevent exfiltration of Company's data from your systems.

The CEC does not wish to provide any more detail on these controls than already provided in the responses above.

Additional Response

After submitting the above comments, members of WSPA raised concerns about a cybersecurity-related document they found on California Department of Technology's (CDT) website, SIMM 5300-C Cybersecurity Maturity Metrics. Members were concerned that the document appeared to publicly disclose sensitive information on security weaknesses and vulnerabilities.

The CEC has reviewed this document and confirmed with CDT that it does not contain data or information on any State system. The document is a form used by State departments to evaluate and report on their cybersecurity maturity, and the version of the form available on CDT's website is a template populated with dummy data to demonstrate how the form should be used.