From: Violeta Navarro

To: TACs and IT POCs

Date: September 28, 2022

Subject: 2022 FBI CJA IT Audit Findings

Hello All,

The Federal Bureau of Investigation (FBI) audit team visited our state in June/July of this year to conduct the required triennial IT audits. The FBI visited 21 local agencies as well as the CJIS Systems Agency (CSA), the Washington State Patrol. We received the final compliance report with the following found as compliance areas for our state as a whole:

1. **Private Contractors:** Ensure the Criminal Justice Information Services (CJIS) Security Addendum is adequately documented, implemented, and signed with all private contractor personnel.
    a. A CJIS Security Addendum is required for private contractors performing a criminal justice function (such as IT, unescorted shredding company personnel, etc.) It must be signed by each vendor employee that has unescorted access to CJI and maintained by the TAC for audit purpose. The CJIS Security Addendums can also be uploaded to CJIS Online.
    b. Refer to the CJIS Security Policy 5.1.1.5 – Private Contractor User Agreements and CJIS Security Addendum
    c. Refer to the ACCESS Operations Manual Chapter 1 – Introduction Private Contractor User Agreements

2. **Personally Owned Information Systems:** Ensure the specific terms and conditions are documented for the use of personally owned information systems with access to Criminal Justice Information (CJI).
    a. Refer to the CJIS Security Policy 5.5.6.1 – Personally Owned Information Systems

3. **Identification/User ID**: Ensure all account management, identification policies, and procedures are implemented on system accounts accessing CJI. (*This was a finding during the previous cycle.*)
    a. Refer to CJIS Security Policy 5.5.1 – Account Management
    b. A procedure is required. A template is available on the FBI website (coming soon to the ACCESS webpage)
    c. We will start reviewing this procedure during our IT audits starting in 2023

4. **Event Logging:** Ensure audit and accountability controls are implemented on information systems accessing CJI. (*This was a finding during the previous cycle.*)
    a. Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern behavior.
    b. Audit logs are required to be retained for at least 365 days and reviewed at least once a week. Refer to CJIS Security Policy 5.4 – Auditing and Accountability

c. Additionally agency's information systems shall provide alerts to appropriate agency officials in the event of an audit processing failure. Refer to CJIS Security Policy 5.4.2 – Response to Audit Processing Failures

5. **Advanced Authentication:** Ensure advanced authentication is implemented for personnel who access or manage information systems accessing CJI from non-secure locations. (*This was a finding during the previous two cycles.*)
    a. Refer to CJIS Security Policy 5.6.2.2 – Advanced Authentication

6. **Encryption:** Ensure CJI transmitted or stored outside the boundary of the physically secure location is immediately protected via encryption to comply with CJIS Security Policy requirements. (*This was a finding during the previous two cycles.*)
    a. Refer to CJIS Security Policy 5.10.1.2 – Encryption

A separate email report will be sent to the agencies that were cited with compliance issues from the FBI. A local agency response is required.

If you were not audited by the FBI please use the above information as a self-assessment to ensure that your agency is following proper policies. Thank you for the efforts you and your agency make to comply!

If you have any questions please let me know.

Thank you,

Violeta Navarro
Information Security Officer
ACCESS Section
Washington State Patrol
Office: 360-534-2161 VoIP: 16161
Mobile: 360-485-9807
ACCESS Webpage