

From: Violeta Navarro
To: NCJA TACs
Date: September 19, 2022
Subject: 2022 FBI NCJA IT Audit Findings

Hello All,

The Federal Bureau of Investigation (FBI) audit team visited our state in June of this year to conduct the required triennial IT audit. The FBI visited 9 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. **Contracted Non-Criminal Justice Services:** Ensure the outsourcing standard is approved and implemented prior to executing a contract or written agreement with a private contractor. Audit Finding: The following local agencies did not request or receive written permission from the State Compact Officer or Chief Administrator prior to outsourcing noncriminal justice functions which allowed contractor personnel unescorted access to Criminal History Record Information (CHRI).
 - a. Please refer to the [ACCESS Operations Manual Chapter 21 – NCJA](#) for guidance on Outsourcing
 - b. Please refer to our [Outsourcing Agreement](#) and [Outsourcing Request to CSA](#) for additional information
2. **Personally Owned Information Systems:** Ensure the specific terms and conditions are documented for the use of personally owned information systems with access to CHRI. Audit Finding: An agency allowed the use of a personally owned information system to access, process, store, or transmit CHRI via the shared file without established and documented procedures.
 - a. Please 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 CHRI. Audit Finding: The following local agencies did not have a written policy to document the validation process of system accounts which access CHRI.
 - a. Please refer to the CJIS Security Policy 5.6.1 – Identification Policy and Procedures
4. **Authentication:** Ensure passwords used for authentication follow secure password attributes. (This was a finding during the previous cycle.) Audit Finding: The Washington State Patrol allowed both local criminal justice and noncriminal justice agencies to utilize shared passwords to decrypt e-mail attachments, which contained CHRI. In addition, the non-unique passwords did not meet the Criminal Justice Information Services (CJIS) Security Policy password requirements. After the audit, it was discussed when everyone is migrated to the new web portal, this issue will be fixed.

- a. Since the audit the WSP has fully migrated to the Web Portal for agencies to receive CHRI. If your agency still doesn't have a Web Portal account please fill out the [application](#) and return per the instructions on the form
5. **Event Logging:** Ensure audit and accountability controls are implemented on information systems accessing CHRI. (This was a finding during the previous cycle.) Audit Finding: An agency did not review audit logs, at a minimum of once a week, for inappropriate, unusual, or suspicious activity.
- a. Please refer to the CJIS Security Policy 5.4.3 – Auditing Monitoring, Analysis, and Reporting

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 and procedures. We recognize the efforts agencies have made to comply and we thank you for that!

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](#)