**Technical Audit Resource Guide**

What to initially expect in an audit:

* CIB auditors will send typically two emails once an audit has been launched.
	+ 1st email = Audit details (including a password for the audit materials, which is in the second email)
	+ 2nd email = Audit materials (packet includes CIB Agreement, Management Control Agreements, CHRI, ORION/NCIC, PSN List, Records, etc.)
* All audit questionnaires are launched via Peak Performance/CJIS Audit software tool. Once those questionnaires are launched, your agency will start receiving automated notifications from the software via email.
* The link for CJIS Audit/Peak Performance is <https://wisconsin.cjisapps.com/cjisaudit/>.
* Most agencies will receive two audit questionnaires (one technical and one TIME). S ORIs and District Attorney offices will only receive TIME questionnaires.
* Note: If your agency is receiving an onsite audit, you will be notified in your initial emails from your auditor. You will still need to submit your agency response to the questionnaires through CJIS Audit. CIB will reach out after the questionnaires have been submitted to schedule an onsite date.

CIB provides audit resources and sample documents on WILENET via: <https://wilenet.widoj.gov/cib/time-system-audits>. Scroll to the bottom of the page for the Audit Documents.

**CIB Audit Process** = PowerPoint presentation that explains the audit process (provides reasons for audits, screenshots from CJIS Audit, sample materials, benefits of audits, etc.)

**CJIS Security Policy Updates – 2024** = PowerPoint presentation from the annual CIB Conference that went over some of the recent updates of the CJIS Security Policy

**CJIS Sample Policies:** This document is a list of sample policies that the CJIS Security Policy requires. Agencies can take these samples and make them their own.

**Sample FIPS Certificate:** Just an example of what a FIPS certificate looks like

**Sample Agency Agreement:** This agreement is for direct access agencies sharing information with indirect access agencies. Any ORI that is sharing information with another ORI will need to have one of these in place and it should be specific to your agencies.

**Management Control Agreement:** This agreement is for non-criminal justice entities (IT Support, Offsite Dispatch Centers (N ORIs), Pre-trial services, etc.) to sign as well as the Criminal Justice Agency with whom they are working.

**Sample TIME System Policy:** This 40+ page document has verbiage that can be used by agencies looking to write policies on things such as validation, hit confirmation, security awareness, access control, etc.

**Sample Network Diagram:** Every agency accessing the TIME System must have a network diagram showing all of their connections and equipment, etc. CIB created a sample that agencies can use to get an idea of what that might look like. The CJIS Security Policy has additional sample diagrams as well.

**CJIS Security Policy -** All technical questionnaires are based on controls from the latest version of the CJIS Security Policy. Your agency IT or LASO should be referencing the policy while going through the questionnaire: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>

**Requirements Companion Document -** the latest version of the document allows agencies to see a summarized versions of the CJIS Security Policy controls and their sanction by dates: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/requirement-companion-document-pdf/view>

**Links of Importance:** The FBI has added several links of importance on their page: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/fbi-cjis-security-policy-resource-center-links-of-importance>. Some of the links included are: IJIS CJIS Security Policy Webinars, Grants.gov, NIST Publications, etc. Click on the link provided for the all-inclusive list.

**FIPS Certificates**: Equipment within agency networks must be encrypted to the appropriate FIPS (Federal Information Processing Standard) level (140-2 acceptable until September 30th, 2026, and then 140-3). To view the status of FIPS certificates, agencies can use the Computer Security Resource Center Cryptographic Module Validation Program to search certificate numbers or vendor/module names. Sometimes Advanced searches are necessary to find historical certificate numbers: <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>.