



CJIS SECURITY LISTSERV

TXDPS Crime Records Division – Compliance & Training Bureau

Website: <https://www.dps.texas.gov/section/crime-records/welcome-tx-cjis-security-office>

Don't feel comfortable clicking links? Copy and paste the URL into a new browser.

CJIS Security Policy v6.0 Local Agency Roles and Responsibilities

Terminal Agency Coordinator (TAC)

Each Agency that interfaces to TLETS is required to have at least one TAC.

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

If an agency wants to assign multiple TAC's, the agency has the discretion to do so. The TAC('s) should be designated on the agency Terminal Connection Report (TCR) that is maintained by TLETS. To update the TCR, please contact TLETS and ask for the TAC-Admin Change Form.

Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

Contracting Agency (CA)

A CA is an agency, whether a CJA, NCJA (public), or NCJA (private), that enters into an agreement with a private contractor subject to the CJIS Security Addendum, The Security and Management Control Outsourcing Standard for Non-Channelers, of the Security and Management Control Outsourcing Standard for Channeling. The CA entering into an agreement with a contractor shall appoint an Agency Coordinator.

Agency Coordinator (AC)

An AC is a staff member of the CA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff as consistent with the NCIC policy.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

Interface Agency (IA) Official

The IA Official is an employee of the IA responsible for planning necessary hardware, software, funding, and training for the IA's authorized access to the CJIS Division's systems. The IA Official shall not be a contract employee.

~~Local Agency Security Officer (LASO)~~

This agency LASO designation has been replaced with eighteen formal designations of Organizational Personnel with Security Responsibilities (below) that must be assigned at each agency. Each of these designations have requirements as stated in each of the Security Control Families under the -1 Policy and Procedures.

Organizational Personnel with Security Responsibilities (formerly LASO)

Each Organizational Personnel with Security Responsibilities shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

There are three “-1 Policy and Procedures” controls that are currently sanctionable for audit, and the auditors will be expecting to see formal documented agency Policy and Procedures to support these control families:

AU – Auditing and Accountability [Existing] [Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.

IR – Incident Response [Existing] [Priority 2]

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures.

MP – Media Protection [Existing] [Priority 2]

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures.

The remaining “-1 Policy and Procedure” controls are not sanctionable for audit until October 1, 2027:

AC (Access Control) – [AC-1 Priority 2]

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures.

AT (Awareness & Training) [AT-1 Priority 2]

Designate organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures.

CA (Security Assessment & Authorization) [CA-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures.

CM (Configuration Management) [CM-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the configuration management policy and procedures.

CP (Contingency Planning) [CP-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the contingency planning policy and procedures.

IA (Identification & Authentication) [IA-1 Priority 2]

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.

MA (Maintenance) [MA-1 Priority 2]

Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the maintenance policy and procedures.

PE (Physical & Environmental Protection) [PE-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures.

PL (Planning) [PL-1 Priority 2]

Designate organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures.

PS (Personnel Security) [PS-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the personnel security policy and procedures.

RA (Risk Assessment) [RA-1 Priority 2]

Designate organizational personnel with security and privacy responsibilities to manage the development, documentation, and dissemination of the risk assessment policy and procedures.

SA (System & Services Acquisitions) [SA-1 Priority 2]

Designate organizational personnel with information security responsibilities and organizational personnel with system and services acquisition responsibilities to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures.

SC (System & Communications Protections) [SC-1 Priority 2]

Designate organizational personnel with information security responsibilities to manage the development, documentation, and dissemination of the system and communications protection policy and procedures.

SI (System & Information Integrity) [SI-1 Priority 2]

Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures.

SR (Supply Chain Risk Management) [SR-1 Priority 2]

Designate organizational personnel with security responsibilities to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures.

Newsletter Update

The current [Ouch! newsletter](#): “[Sweet Talk and Empty Wallet: Romance Fueled Investment Scams](#)” Read “A story to remember: Lisa’s Experience”, a story of betrayal and loss. Learn what “Pig Butchering” is, how to detect it, and to protect yourself.

Resource Roundup [FBI's Law Enforcement Enterprise Portal \(LEEP\)](#) provides LE agencies, intelligence groups, and criminal justice entities access to web-based investigative tools and analytical resources.

Cybersecurity & Infrastructure Security Agency (CISA) provides current [Cybersecurity Alerts & Advisories](#) to help detect and mitigate vulnerabilities.

[Multi-State Information Sharing & Analysis Center \(MS-ISAC\)](#) provides cybersecurity webinars, newsletters, and advisories on known vulnerabilities in popular software free for (State, Local, Tribal, and Territorial) SLTT entities.

Texas Department of Information Resources – (TX DIR) – provides resources to Texas governmental entities to help collaborate and share technical resources, join mail lists from Texas Information Sharing and Analysis Organization (Tx ISAO) and

more on [DIR's Collaboration Page](#). You can also access the [Texas Risk and Authorization Management Program \(TX-RAMP\)](#).

DPS Cyber Security Team also provides [Cyber Security Newsletters](#) on the DPS website.

Thank you for subscribing to the CJIS Security Office Technical listserv.

We truly appreciate you.