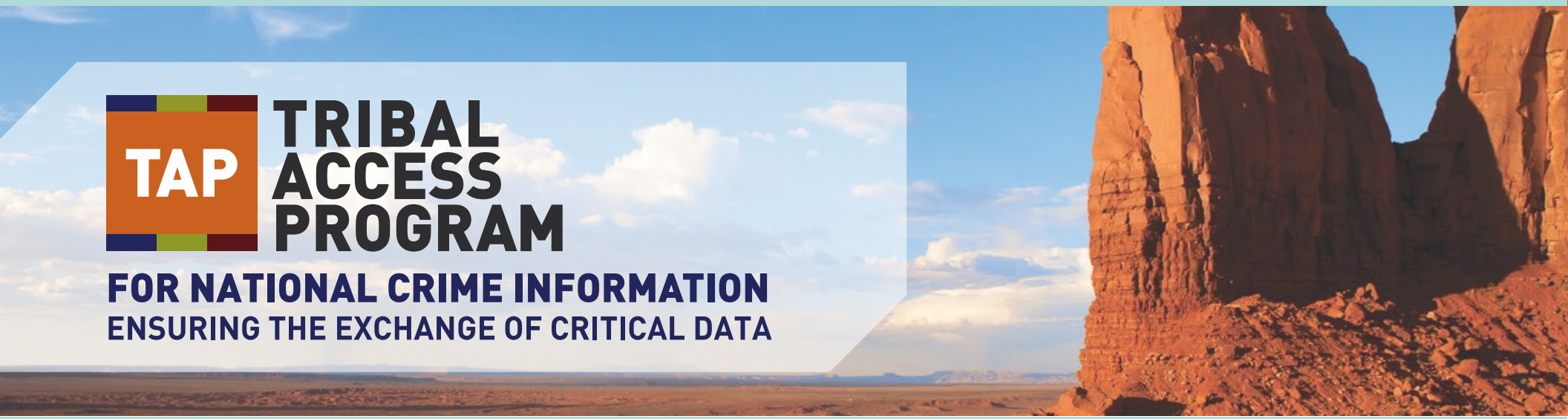

Terminal Agency Coordinator (TAC) Duties and Responsibilities

Department of Justice
Office of the Chief Information Officer
Office of Tribal Justice

WEB: WWW.JUSTICE.GOV/TRIBAL/TAP
EMAIL: TRIBALACCESS@USDOJ.GOV

Objectives

- Understand TAC roles and responsibilities pre- and post-deployment
- Understand CJIS Security Policy requirements related to the TAC's role

What is a Terminal Agency Coordinator (TAC)?

- Terminal Agency Coordinator (TAC) is a role required by the FBI Criminal Justice Information Services (CJIS) Security Policy
  - Must be one for each agency that has access to CJIS systems
  - Serves as the Tribal agency point-of-contact on matters relating to access to FBI CJIS systems
- Responsible for ensuring agency compliance with policies and procedures of:
  - FBI CJIS Security Policy
  - CJIS system-specific policy manuals
- Can delegate specific responsibilities

What can a TAC Delegate?

- TACs are permitted to delegate certain responsibilities, which include:
  - Local Agency Security Officer (LASO)
  - N-DEX Agency Coordinator (NAC)
- TAC maintains accountability for delegated responsibilities
- Must maintain a current list of personnel with scope and dates of delegated responsibilities

Pre-Deployment Responsibilities

- Prepare ORI request for agency
- Ensure agency users meet minimum screening requirements
  - Complete Agency User Spreadsheet with all agency employees (who have unescorted access to CJI) and indicate which users will be taking fingerprints and which will be NCIC users
- Ensure applicable agency users apply for a LEEP account or N-DEx accounts
- Submit JCIS documentation
- Ensure agency understands and adheres to proper use of handling Criminal Justice Information (CJI)

Prepare ORI Request for Agency

- Attend Webinars
  - How to complete an ORI Request Package for CJA
  - How to complete an ORI Request Package for Non-CJA
- See ORI Checklists and ORI Request Samples for LE-CJA, Non-LE CJA and Non-CJI on Onboarding and Vetting website
- Gather required documents into a single PDF
- Submit ORI Request to BRM and cc: tribalaccess@usdoj.gov

User Accounts: Minimum Screening Requirements

- Ensure agency users meet minimum screening requirements and complete training and certifications prior to deployment
  - CJIS Security Awareness Test (CSAT)
  - NCIC Certification Test (Only for “Hands on” users)
  - Fingerprint-based criminal records check within the past 5 years
- Complete Agency User Spreadsheet with all agency employees (who have unescorted access to CJI)
  - Indicate which users will be taking fingerprints and which will be NCIC users and return to Primary POC
- Primary POC shall aggregate all Agency User Spreadsheets and send the aggregated version to the BRM
- TAP will not schedule a deployment until 80% of all users have taken and passed CJIS SAT and NCIC training

User Accounts: LEEP and N-DEx

- A LEEP account is required for:
  - Access to the National Data Exchange (N-DEx)
  - Ability to submit fingerprints to Next Generation Identification (NGI)
  - Secure email for users to exchange CJI (e.g. criminal history) between agencies
  - TACs should ensure that agency users apply for a LEEP account and monitor the application process
  - TACs must notify the TAP team once accounts are created
- If participating in N-DEx, TAC supports:
  - Tribe in submitting logo
  - Identifying a N-DEx moderator (if different from the TAC)
  - Ensuring N-DEx moderator signs the NAC Addendum

Complete and Submit JCIS Documentation

- TAC is responsible for assisting their agency in completing and submitting JCIS documentation
  - The TAC for each agency must sign the agreement
  - When new TACs are assigned, the agreement must be updated
- Documentation required varies based on responsibilities, agency relationships, and usage
  - TAP User Agency Agreement
  - TAP Addendum
  - Terminal Agency Coordinator Addendum
  - Local Agency Security Officer Addendum
  - National Data Exchange Coordinator Addendum
  - Information Exchange Agreement
  - Information Protection Agreement

Post-Deployment Responsibilities

- Manage user accounts
- Ensure data quality of NCIC records
- Ensure correct fingerprint submission process is used
- Ensure agency policies regarding CJI are current
- Participate in metric calls
- Participate in FBI CJIS and DOJ audits

User Accounts, Training, and Certification

- TACs are responsible for ensuring agency user accounts are current
- CJIS Security Awareness Training (CSAT)
  - Add, modify, or deactivate new user accounts (through www.cjisonline.com)
  - Ensure user's recertification every 2 years
- OpenFox Messenger (OFM)/NCIC
  - Request new NCIC user accounts by submitting a request to the DOJ Service Desk with:
    - User's full name, agency, email address and phone number and
    - Indicate if they are querying/entering person or property files and/or submitting fingerprints
  - Notify DOJ Service Desk when a NCIC accounts need to be modified and/or deactivated
  - Ensure user's recertification every 2 years

Data Quality of NCIC Records

- TACs must ensure that there is a policy in place for data quality to include:
  - Timely entry, modification and removal of records (ongoing)
  - Second party verification (upon entry)
  - Record validation (monthly)
  - 24 x 7 hit confirmation

Fingerprint Submission Process

- If agency submits fingerprint transactions, TAC must:
  - Ensure agency uses correct workflow (FAUF or FANC)
  - Ensure proper “Reason Fingerprinted” is used
  - Ensure fingerprinted persons are given, sign, and return the “Notice and Consent” form
  - Ensure Information Exchange Agreements (IEA) are in place and up to date if identity history summaries (IdHS) are provided to another agency

Agency Policies Regarding CJI

- TACs must ensure agency policies regarding the handling of Criminal Justice Information (CJI) are created and remain update
- Examples of policies include:
  - Policy and procedure for keeping training accounts up to date, which would include procedures for removing an account is staff were to leave or add a new account for new employees
  - Policy for responding to hit confirmation requests
  - Policy for entering and validating information into NCIC, to include second party checks, initial validation, and annual validation
- DOJ/TAP team is currently developing policy templates to assist Tribes in developing procedures for all TAP related activities in the Agency

Metric Calls with TAP Team

- TACs must attend metric calls with TAP team
  - Provides an overview on the agency's use
  - Identifies opportunities for training from TAP team
- TACs follow up with agency on action items identified from the metric meetings

Participate in FBI CJIS and DOJ Audits

- TACs are responsible for participating in audits by:
  - Completing audit questionnaires
  - Attending in-person audits, and
  - Ensuring corrective action is taken if there are audit findings
- TACs are required to attend DOJ TAP team audit-related webinars for awareness on requirements

Replacing a TAC

- Tribe needs to contact TAP team with the new TAC's contact information
- Users new to the TAC role should:
  - Complete CJIS SAT and if applicable, NCIC training/certification
  - Sign Terminal Agency Coordinator Agreement
  - Sign and resubmit new:
    - TAC Addendum
    - TAP Addendum
    - Information Exchange Agreement
    - Information Protection Agreement

Resources

- Training and reference materials can be found in the CJIN Training and Learning Portal
  - https://nextest.just.jmd.usdoj.gov/cjin/index.php
- Contact your Tribe's assigned Business Relationship Manager (BRM) by email with questions
  - Cc: tribalaccess@usdoj.gov
  - Please include your Tribe's name in the subject line of the email
- Technical questions and inquiries should be sent to the Idemia Help Desk
  - For urgent requests, please call 800-734-6241
  - Routine requests can be sent by email to CSCenter@idemia.com
    - Cc: tribalaccess@usdoj.gov
    - Please include your Tribe's Name in the subject line of the email