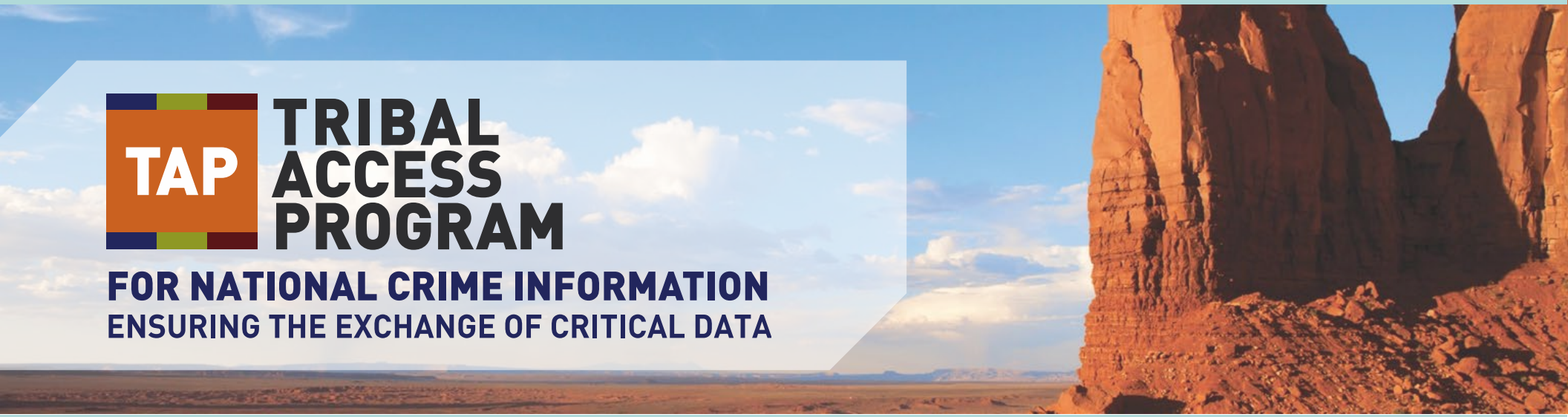



# Terminal Agency Coordinator (TAC) Duties and Responsibilities

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

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

# Webinar Presenter

**YOUR INSTRUCTOR**
Bradley Colquitt
Lead Business Relationship Manager (BRM)
Tribal Access Program (TAP)
Bradley.S.Colquitt@usdoj.gov
202-616-0707

My name is Brad Colquitt and I've been a member of the TAP team since the beginning of the program in October of 2015. I am responsible for oversight of TAP BRMS and Trainers, as well as onboarding and vetting, deployment & training, and post deployment support of TAP Tribes. Prior to joining TAP, I have worked in Federal IT projects for numerous government agencies. I have over 30 years' experience in Information Technology consulting, planning, and implementation for various branches of the U.S. government.

# Webinar Presenter

**YOUR INSTRUCTOR**
Jose H. Primera Jr.
Training Coordinator/DOJ
Tribal Access Program (TAP)

Email: Jose.Primera@usdoj.gov
Telephone: (202) 532-5186

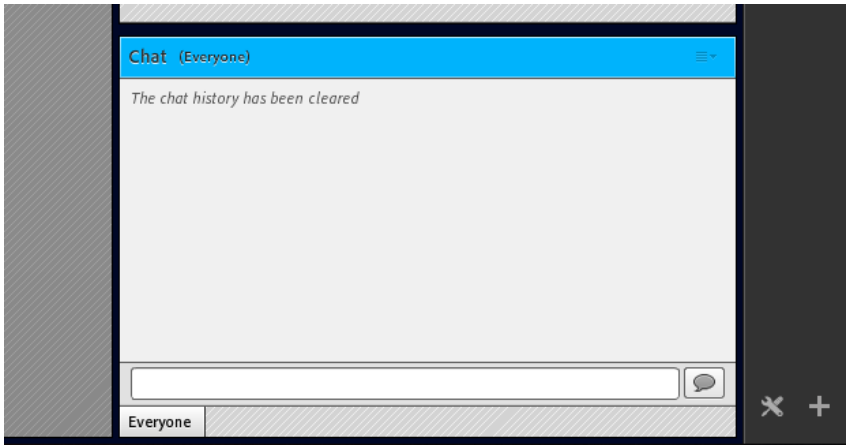
Hi, I'm Jose Primera and I'll be your instructor for this Webinar. I am the lead Federal Training Instructor with the United States Department of Justice assigned to the Office of the Chief Information Officer within the Justice Management Division in Washington DC. I specialize in NCIC/ NLETS and JUST Training of Federal agents. I am currently detailed to the Department's Tribal Access Program that provides NCIC, III and NLETS access to Native American Tribal Police and Civil Agencies. I have a degree in Criminal Justice and enjoyed an active law enforcement and training career for over 35 years.

My training and law enforcement career has included 11 years with the Texas Alcoholic Beverage Commission, Seven of which were in the Training Division at headquarters in Austin, Texas; where I was promoted through to the rank of Lieutenant. My background also includes 12 years with the Midland County Sheriff's Office, where I played a key role in narcotics and undercover investigations. I currently hold a Deputy Sheriff's Commission.

# Webinar Housekeeping

- **Audio**
  - Join webinar audio by phone
  - Dial the conference call number provided in the calendar invitation
  - Enter the access code provided in the calendar invitation when prompted
  - All participants should MUTE their phone
  - Do not place your phone on hold

- **Attendance**
  - To ensure that we have a record of your attendance, type your name and your Tribe's name in the Chat window




- **Questions**
  - Questions may be typed in the Chat window or verbally asked during the question and answer period of the webinar

# Objectives

- Background and Context
  - FBI CJIS, DOJ as CSA, and the DOJ Justice Criminal Information Services (JCIS)
- What is a TAC?
- User Agency Agreement and TAC Addendum
- TAC Roles and Responsibilities
- Pre-deployment TAC Activities
- Post-deployment TAC Activities
- TAC Resources

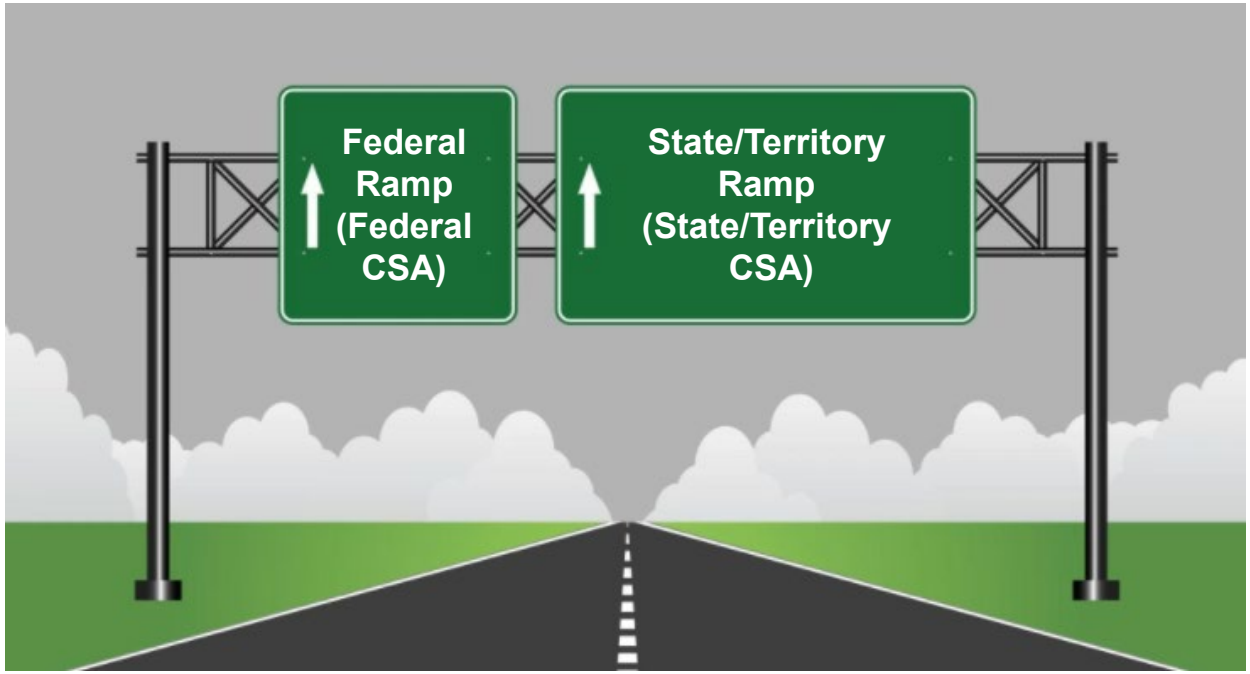
# Overview of the DOJ CSA:
# DOJ Justice Criminal Information Services

# FBI & Criminal Justice Information

- FBI Criminal Justice Information Services (FBI CJIS) houses Criminal Justice Information submitted by State, Local, and Federal Agencies nationwide with limited Tribal participation prior to TAP
- Located in Clarksburg, WV

- FBI Criminal Justice Information Systems:
  - National Crime Information Center (NCIC)
  - Interstate Identification Index (III)
  - Next Generation Identification (NGI)
  - National Instant Criminal Background Check System (NICS)
  - National Data Exchange (N-DEx)

# Access to Criminal Justice Information




- There is only one way for authorized federal, state/territory, local, and Tribal agencies to access the FBI CJIS systems: through a CJIS Systems Agency (CSA)
- There are two types of CSAs: federal or state/territory
- Each federal or state/territory CSA sets its own rules, regulations and policies

# DOJ Justice Criminal Information Services

- DOJ CSA facilitates access to the national crime information systems through the following Justice Criminal Information Services (JCIS; formerly known as Criminal Justice Information Network – CJIN):
  - **Joint Automated Booking System (JABS)** – securely provides authorized agencies with query and submission capability in the FBI CJIS NGI system, a database of palmprints, fingerprints, iris, and mugshots
  - **Civil Applicant System (CAS)** – securely provides authorized agencies the capability to electronically capture and submit fingerprints to the FBI CJIS NGI system for expedited national Identity History Summary checks for non-criminal purposes, such as employment and national security clearances
  - **Justice Web Interface to NCIC (JWIN)(**formerly known as Justice Telecommunications System) – securely provides authorized agencies access to the NCIC and III, NICS, and NIets
- Additionally, the DOJ CSA will facilitate access to the National Data Exchange (N-DEx) System, an investigative information sharing system that contains incident, arrest, and booking reports, pretrial investigations, supervised released reports, calls for service, photos, and field contact/identification records.

# What is a Terminal Agency Coordinator (TAC)?

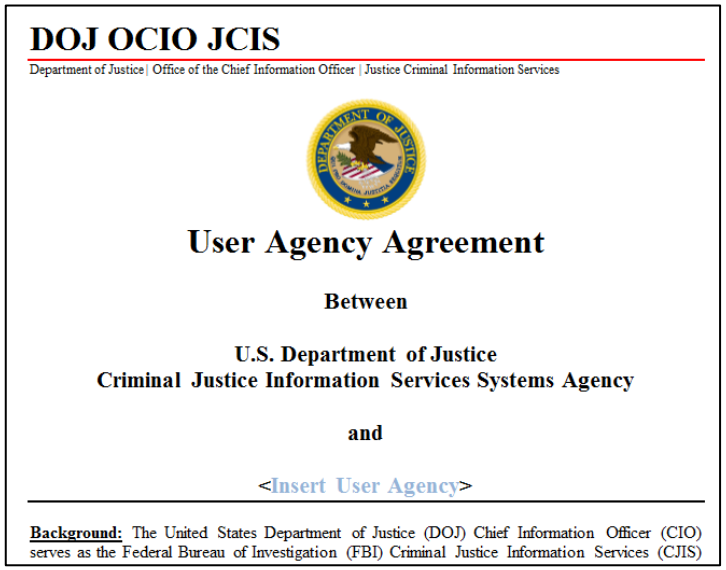
- Terminal Agency Coordinator (TAC) is a role required by the FBI Criminal Justice Information Services (CJIS) Security Policy
  - Must be one for each agency that has access to CJIS systems
  - Serves as the Tribal agency point-of-contact on matters relating to access to FBI CJIS systems
- Responsible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

# User Agency Agreement and Addenda

# User Agency Agreement and TAC Addendum

- The User Agency Agreement and TAC Addendum outline the responsibilities of the DOJ CSA and the User Agency, with regard to access to the FBI CJIS systems

  The User Agency shall appoint an Executive to sign the **User Agency Agreement (UAA)** with the DOJ CSA. The User Agency Executive is the accountable party for the User Agency and enforces the FBI CJIS Security Policy and DOJ CJIN Policy over its user community.



DOJ OCIO JCIS

Department of Justice | Office of the Chief Information Officer | Justice Criminal Information Services

**User Agency Agreement**

**Between**

**U.S. Department of Justice**
**Criminal Justice Information Services Systems Agency**

**and**

<Insert User Agency>

**Background:** The United States Department of Justice (DOJ) Chief Information Officer (CIO) serves as the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)

DOJ OCIO JCIS

Department of Justice | Office of the Chief Information Officer | Justice Criminal Information Services

**User Agency Agreement**
**Terminal Agency Coordinator (TAC)**
**Addendum**

**Between**

**U.S. Department of Justice**
**Criminal Justice Information Services Systems Agency**

**and**

<Insert User Agency>

**Purpose:** This Addendum to the User Agency Agreement sets forth the responsibilities of the Terminal Agency Coordinator (TAC) for the protection of Criminal Justice Information (CJI) accessed through the DOJ Justice Criminal Information Services (JCIS). All acronyms not defined herein have the meaning given in the User Agreement.

The User Agency Executive must appoint a TAC to carry out the responsibilities described in the User Agency Agreement and **TAC Addendum**. The User Agency Executive must notify the DOJ CSA of any changes to the TAC role, as a new TAC Addendum must be signed

# TAC Addendum – Roles and Responsibilities

- Each Agency TAC must sign a TAC Addendum, which outlines the roles and responsibilities of the TAC. The TAC shall:
  - Serve as the User Agency point-of-contact for matters relating to FBI CJIS information access, and administer DOJ JCIS programs across the entire User Agency
  - Ensure the User Agency complies with FBI CJIS Security Policy (CSP), related FBI CJIS system-specific manuals, the Nlets User Policy Manual, directives and decisions of the criminal justice community's Advisory Policy Board (APB), National Crime Prevention and Privacy Compact Council, and all relevant DOJ specific policies, orders, and regulations
  - Ensure the User Agency maintains criminal justice record quality, accuracy, availability, and validity
  - Ensure all users with access to CJI meet the appropriate minimum screening, training, and certification requirements prior to access being granted
  - Notify the DOJ CSA of any network, system, or security changes, and the status of personnel within the User Agency that will impact their legal authority for access to CJI

# TAC Addendum – Roles and Responsibilities
*(continued)*

- Notify the DOJ CSA of any suspected or verified misuse of the national crime information systems
- Maintain copies of the signature pages of the FBI CJIS Security Addendum for each contractor employee prior to the contractor employee being granted access to CJI. Copies of the signature page shall be made available at the time of an audit, or upon request from the DOJ CSA
- Maintain and biennially validate the User Agency's Originating Agency Identifiers (ORIs)
- Initiate, maintain, and annually validate user accounts
- Ensure completion of monthly NCIC record validations
- Perform all TAC responsibilities, unless affirmatively delegated to other individuals. While the TAC may delegate responsibility, they may not delegate overall accountability. The TAC must maintain a current list of any delegations, and their effective dates. This list must be made available to the DOJ CSA upon request.

# Other Tribal Roles and Responsibilities

- Although each Tribal agency has a TAC, there are some roles that require a Tribal level POC
- The TAC may discharge or delegate the following DOJ CSA required roles:
  - Local Agency Security Officer (LASO) – the primary Information Security point-of-contact between the User Agency and the DOJ CSA (CSP 3.2.9).
  - N-DEx Agency Coordinator (NAC) – primary N-DEx point-of-contact between the User Agency and the DOJ CSA (N-DEX 1.6.4)
  - Technical Point of Contact (TPOC) – liaison between the User Agency and the DOJ CSA to support technical issues, such as system operability, software and hardware installation, and network/router connectivity

# PRE-DEPLOYMENT Activities

# Pre-Deployment Responsibilities

- Prepare ORI request for agency
- Ensure agency users meet minimum screening requirements
  - On-line Training
  - Fingerprint-based criminal records check every 5 years
- Ensure applicable agency users apply for a LEEP account and/or N-DEx accounts
- Submit JCIS documentation
- Ensure agency understands and adheres to proper use of handling 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-Criminal Justice Agency (NCJA)
- See ORI Checklists and ORI Request Samples for LE-CJA, Non-LE CJA and NCJA 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

# User Accounts: LEEP and N-DEx

- Law Enforcement Enterprise Portal (LEEP)
  - A LEEP account is required to:
    - Submit fingerprints to NGI via an @leo.gov account
    - Access to the N-DEx
    - 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  (Can take up to 4-6 weeks for approval)
  - TACs must notify the TAP team once accounts are created
- National Data Exchange (N-Dex), TAC assists with:
  - Identifying a N-DEx moderator (if different from the TAC)
  - Submitting Tribal logo
  - 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 ensure the TAC, LASO, and NAC addenda are signed
  - When new TACs are assigned, the TAC, LASO, and NAC addenda must be updated
- Documentation required varies based on responsibilities, agency relationships, and usage
  - TAP User Agency Agreement (UAA)
  - TAP Addendum
  - Terminal Agency Coordinator (TAC) Addendum
  - Local Agency Security Officer (LASO) Addendum
  - National Data Exchange Coordinator (NAC) Addendum
  - Information Exchange Agreement (IEA)
  - Information Protection Agreement (IPA)

# POST-DEPLOYMENT Activities

# 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
- Justice Web Interface to NCIC (JWIN)
  - 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 are required
  - Notify DOJ Service Desk when 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
  - 24 x 7 hit confirmation
  - Biennial Validation of ORI

# Fingerprint Submission Process

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

# Fingerprint Submission Process

| Type of Criminal Justice Agency (CJA) Applicant | Select the appropriate Criminal TOT | Select the ORI of the Criminal Justice Agency that the applicant is applying with or employed by | Select Reason Fingerprinted (RFP) | Email address to Submit Prints from your LEEP Account |
|---|---|---|---|---|
| **Criminal Justice Agency personnel working directly for the agency** | Federal Applicant No Charge (FANC) | Law Enforcement (00)<br>Prosecutor (A)<br>Corrections (C)<br>Criminal Court (J)<br>Probation (G)<br>Pretrial Services (B) | 28 CFR 20-33 a 1 | submit@cas.doj.gov |
| **Criminal Justice Agency contractors or vendors that are not under management control of the CJA** | Federal Applicant User Fee (FAUF) | | 28 CFR 20-33 a 7 | |
| **Employees, Prospective Employees, or Volunteers who have contact and control over Indian Children** | Federal Applicant User Fee (FAUF) | Social Services (Z)<br>Human Resources (Z) | Public Law 101-630 | submit@cas.doj.gov |
| **Follow-up Fingerprints for Purpose Code X placements through BIA Program** | Federal Applicant User Fee (FAUF) | Social Services (Z) | Public Law 101-630 Emergency Placement<br>NOTICE: Within 15 calendar days of placement, if the child is still in in the emergency placement, a fingerprint-based record check must be performed on all adult household members. | |
| **Employees or Prospective Employees of Public Housing Agency and Adult applicants or tenants receiving housing assistance for the purposes of screening, lease enforcement or eviction** | | Housing (Q) | 25 USC 4138 | submit@cas.doj.gov |

# Agency Policies Regarding CJI

- TACs must ensure agency policies regarding the handling of CJI are created and remain updated
- Examples of policies include:
  - Policy and procedure for keeping training accounts up to date, which would include procedures for removing an account if 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
  - IT Policy
- DOJ/TAP team has developed policy templates to assist Tribes in developing procedures for all TAP related activities in the Agency

# Metric Calls with TAP Team

- TACs must attend periodic metric calls with TAP team
  - Provides an overview on the agency's use
  - Focus is on low usage areas and reasons (technical, training, other)
  - 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 and resubmit new:
    - Terminal Agency Coordinator Addendum
    - Information Exchange Agreement
    - Information Protection Agreement
    - Other Addenda as required (e.g. NAC and LASO)
  - JCIS Documentation is available online: https://www.justice.gov/tribal/onboarding-and-vetting

# Resources

- Training and reference materials can be found in the JCIS Training and Learning Portal
  - https://csa.justice.gov/launchpad/
- 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 about the kiosk post deployment should be sent to the Idemia Help Desk
  - For urgent requests, please call 800-734-6241
  - Routine requests can be sent by email to AnaheimCSCenter@us.idemia.com
    - Cc: tribalaccess@usdoj.gov
    - Please include your Tribe's Name in the subject line of the email