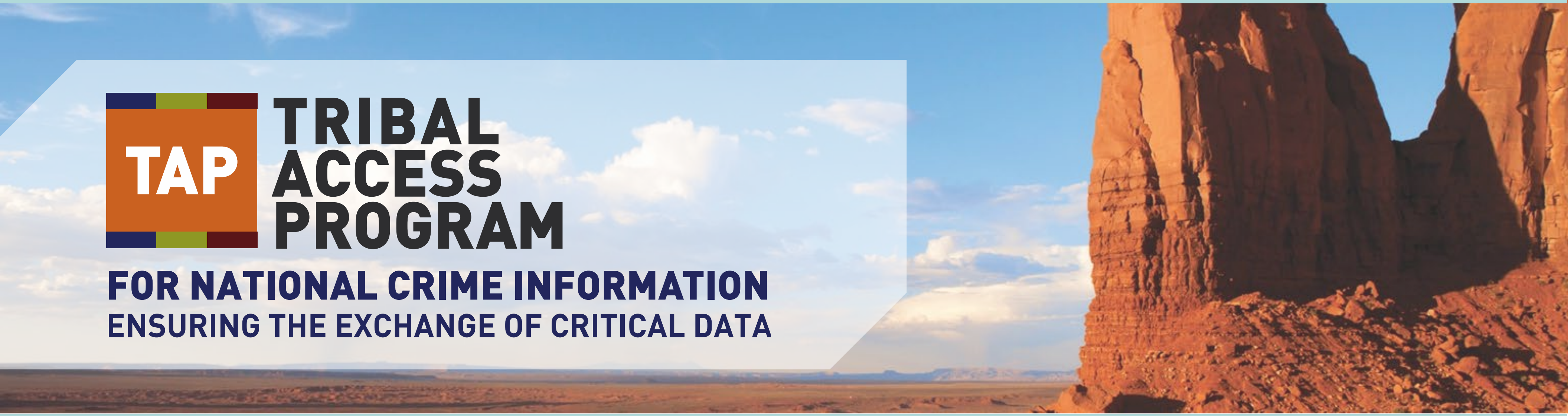


TAP TRIBAL ACCESS PROGRAM

FOR NATIONAL CRIME INFORMATION

ENSURING THE EXCHANGE OF CRITICAL DATA

Terminal Agency Coordinator (TAC) Roles 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

Teams Meeting Housekeeping

WEBINAR (Connection & Navigation)

- Connecting by Computer or Phone
- Navigating Microsoft Teams
  - Control Bar (Click on screen)
    - **Mic | Camera | Raise Hand | Chat**

ATTENDANCE (Chat Window)

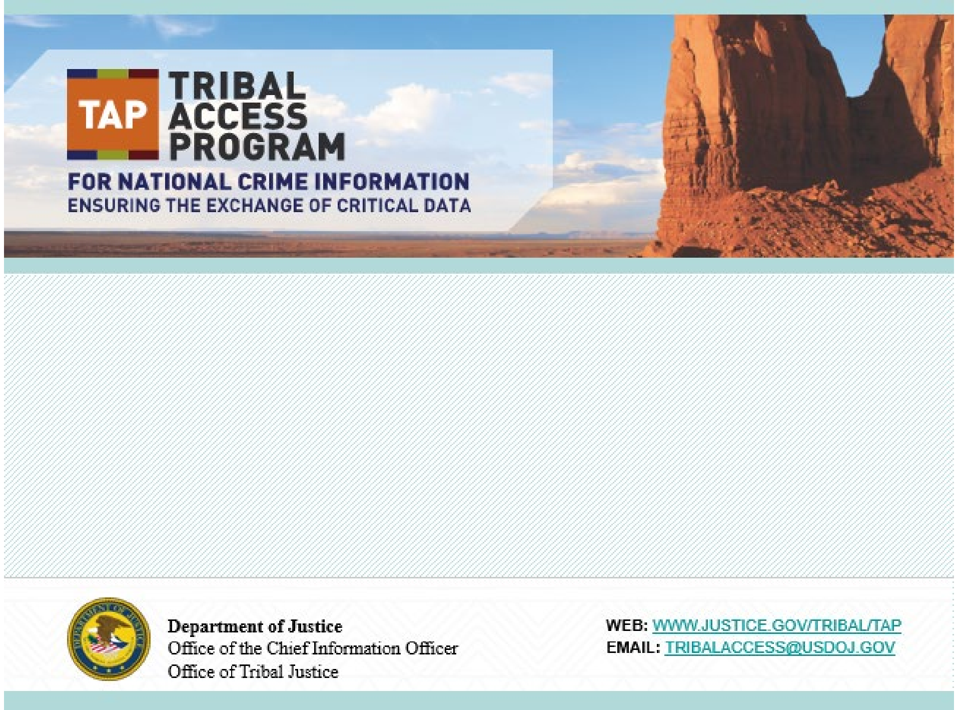
- Name
- Title
- Tribal Agency

QUESTIONS

- Raise Hand | Chat Message | Verbal

SURVEY

- We value your feedback!

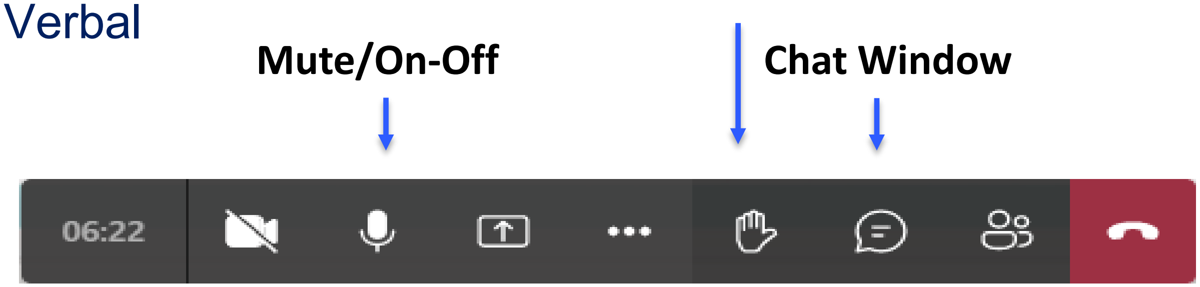


TAP TRIBAL ACCESS PROGRAM

FOR NATIONAL CRIME INFORMATION
ENSURING THE EXCHANGE OF CRITICAL DATA

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

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



Raise Hand

Mute/On-Off

Chat Window

Control Bar

Agenda

- What is a Terminal Agency Coordinator (TAC)
- User Agency Agreement, TAC Addendum, & TAC Responsibilities
- Tribal Level Roles and Responsibilities
- Pre-Deployment TAC Responsibilities
  - JCIS Documents
  - Apply for ORI
  - User Accounts: CSAT and JWIN,
  - Other Accounts: LEEP and N-DEx
- Post-Deployment TAC Responsibilities
  - Data Quality of NCIC Records, Users, & ORIs
  - Tribal and Agency Policies related to CJI
  - Monitoring Fingerprint Transactions
  - Appropriate Use and Participation in Audits
- Training and Reference Materials
- Resources

What is a TAC?

A 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
- Located at Home / JCIS Training and Learning Center (justice.gov)

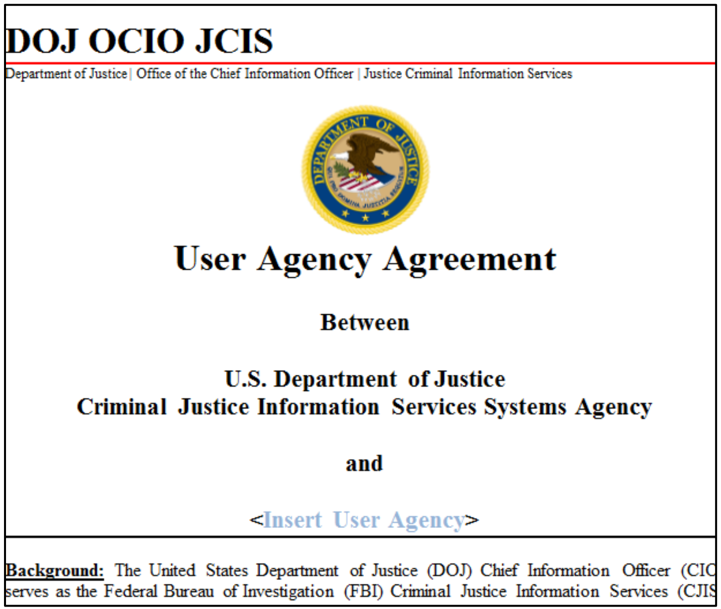
User Agency Agreement & TAC Addendum

User Agency Agreement

- Signed by the agency executive
- The User Agency Executive must appoint a TAC to carry out the responsibilities described in the User Agency Agreement and TAC Addendum

Terminal Agency Coordinator (TAC) Addendum

- Signed by the agency executive and TAC
- May delegate roles and responsibilities
  - If delegating roles, TAC must maintain a current list of delegations and effective dates
  - While the TAC may delegate responsibility, they may not delegate overall accountability
- The User Agency Executive must notify the BRM of any changes to the TAC role
- When a new TAC is assigned a new TAC Addendum must be signed



DOJ OCIO JCIS

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

User Agency Agreement

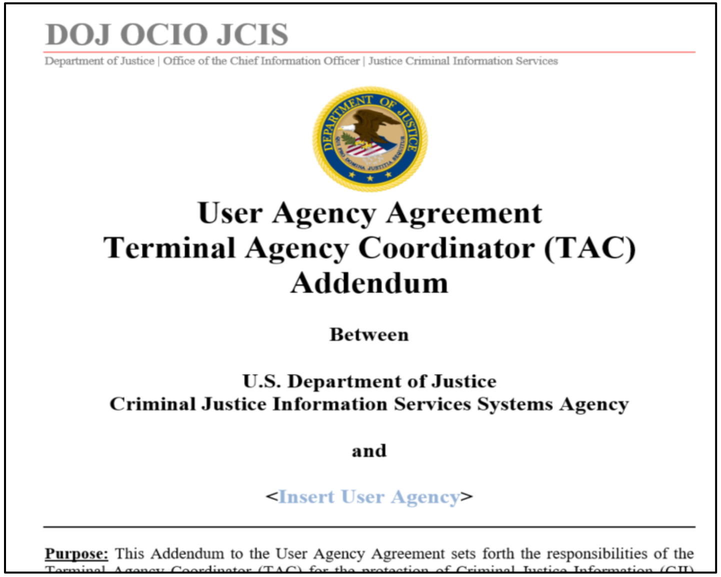
Between

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

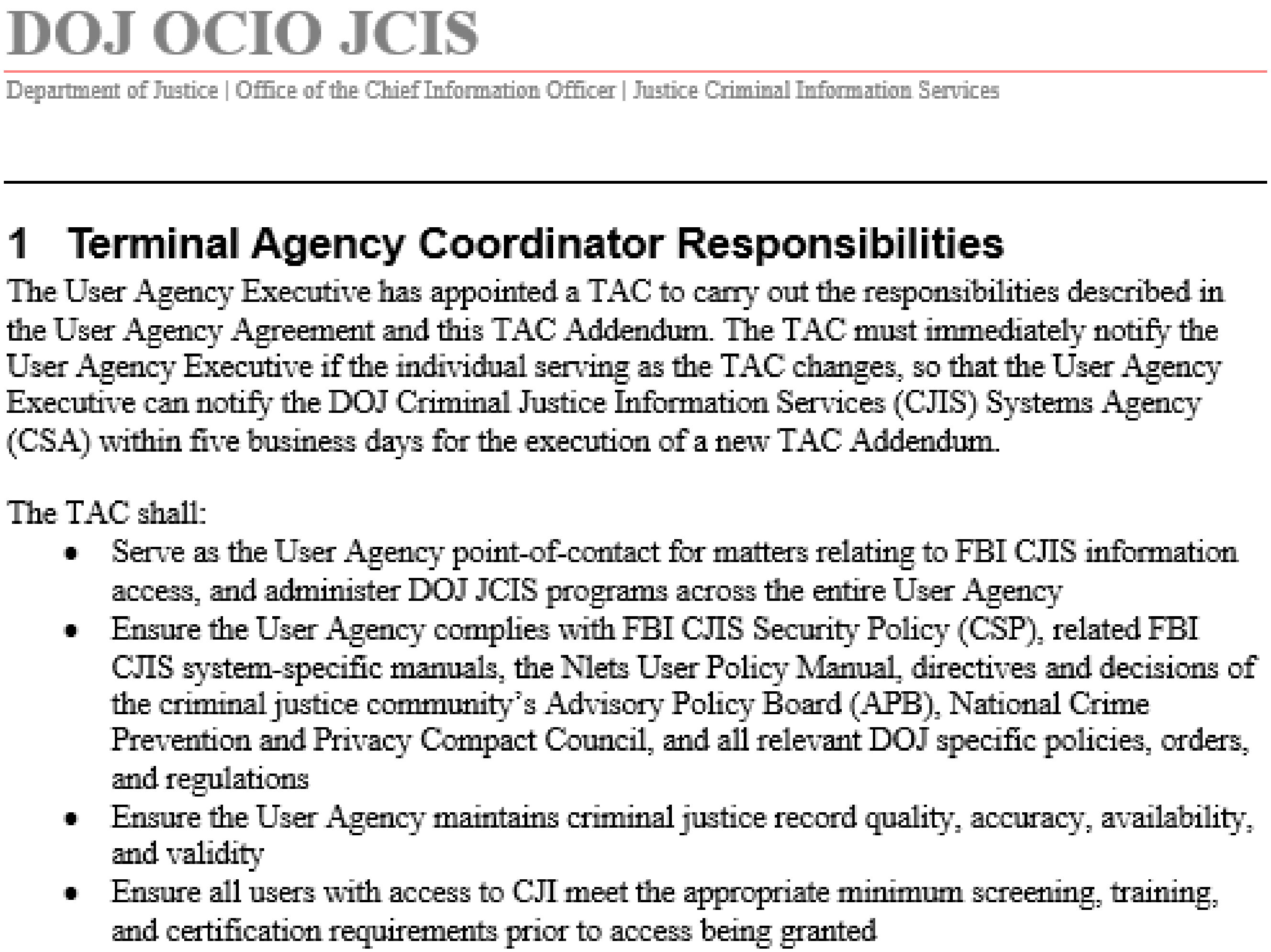
<Insert User Agency>

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)

TAC Responsibilities

Terminal Agency Coordinator (TAC) Addendum

- List 12 responsibilities of the TAC



DOJ OCIO JCIS

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

1 Terminal Agency Coordinator Responsibilities

The User Agency Executive has appointed a TAC to carry out the responsibilities described in the User Agency Agreement and this TAC Addendum. The TAC must immediately notify the User Agency Executive if the individual serving as the TAC changes, so that the User Agency Executive can notify the DOJ Criminal Justice Information Services (CJIS) Systems Agency (CSA) within five business days for the execution of a new TAC Addendum.

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

Tribal Level Roles and Responsibilities

- The following roles are assigned for the Tribe as a whole. Each Agency TAC should be familiar with these roles and who is designated for their Tribe.
  - **Local Agency Security Officer (LASO)** – the primary Information Security point-of-contact between the User Agency and the DOJ CSA (CSP 3.2.9).
  - **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. This person may also be the LASO.
  - **N-DEx Agency Coordinator (NAC)** – primary N-DEx point-of-contact between the User Agency and the DOJ CSA (N-DEX 1.6.4)
  - **LEEP Coordinator –** responsible for sponsoring Non-Criminal Justice Agency employees for LEEP accounts, needed for submitting fingerprints by Human Resources, Housing, or Social Services. The LEEP Coordinator also approves LEEP accounts for Criminal Justice Agencies

Pre-Deployment Responsibilities

Pre-Deployment TAC Responsibilities

Submit JCIS documentation (Agency Level):

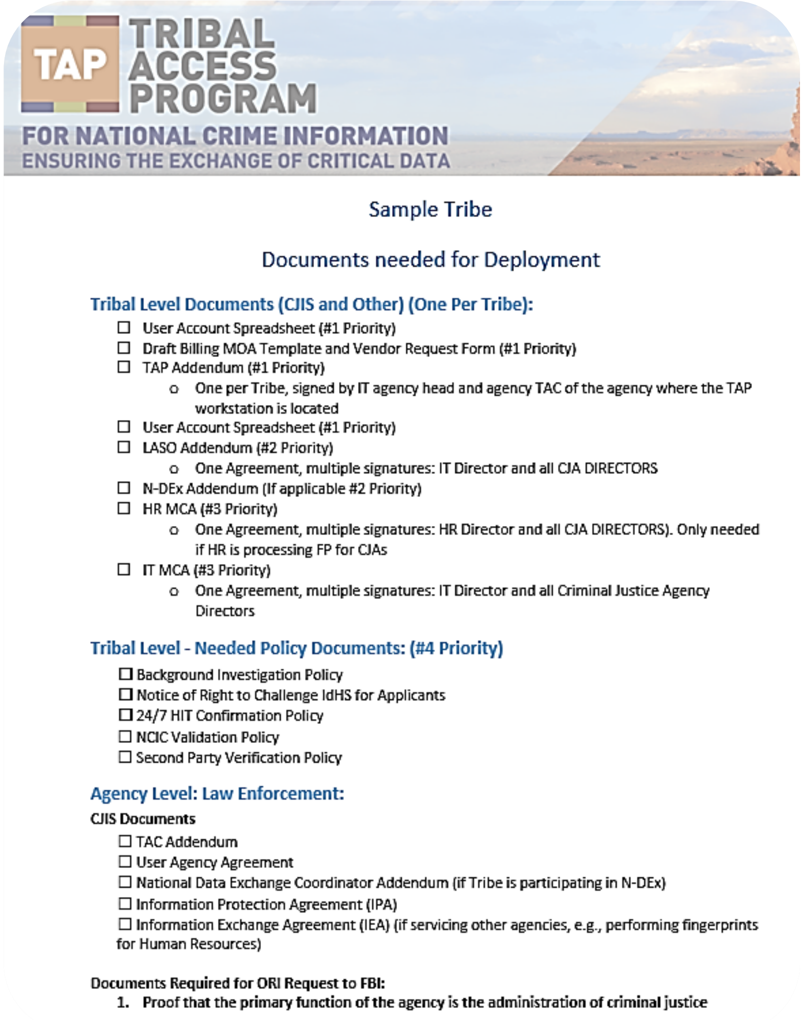
- TAP User Agency Agreement (UAA)
- Terminal Agency Coordinator (TAC) Addendum
- Information Protection Agreement (IPA) or
- Information Exchange Agreement (IEA)

Prepare for ORI request:

- Attend webinars
- Gather required documents
- Submit documents in a single PDF for ORI Request to BRM and cc: tribalaccess@usdoj.gov

Train and Prepare for Access:

- Ensure agency users meet minimum screening requirements
  - On-line Training – Set up training Accounts
- Set up other required accounts
- Ensure agency understands and adheres to the proper use of and handling of Criminal Justice Information (CJI)



TAP TRIBAL ACCESS PROGRAM
FOR NATIONAL CRIME INFORMATION
ENSURING THE EXCHANGE OF CRITICAL DATA

Sample Tribe

Documents needed for Deployment

Tribal Level Documents (CJIS and Other) (One Per Tribe):

- ☐ User Account Spreadsheet (#1 Priority)
- ☐ Draft Billing MOA Template and Vendor Request Form (#1 Priority)
- ☐ TAP Addendum (#1 Priority)
  - One per Tribe, signed by IT agency head and agency TAC of the agency where the TAP workstation is located
- ☐ User Account Spreadsheet (#1 Priority)
- ☐ LASO Addendum (#2 Priority)
  - One Agreement, multiple signatures: IT Director and all CJA DIRECTORS
- ☐ N-DEx Addendum (If applicable #2 Priority)
- ☐ HR MCA (#3 Priority)
  - One Agreement, multiple signatures: HR Director and all CJA DIRECTORS). Only needed if HR is processing FP for CJAs
- ☐ IT MCA (#3 Priority)
  - One Agreement, multiple signatures: IT Director and all Criminal Justice Agency Directors

Tribal Level - Needed Policy Documents: (#4 Priority)

- ☐ Background Investigation Policy
- ☐ Notice of Right to Challenge IdHS for Applicants
- ☐ 24/7 HIT Confirmation Policy
- ☐ NCIC Validation Policy
- ☐ Second Party Verification Policy

Agency Level: Law Enforcement:

CJIS Documents

- ☐ TAC Addendum
- ☐ User Agency Agreement
- ☐ National Data Exchange Coordinator Addendum (if Tribe is participating in N-DEx)
- ☐ Information Protection Agreement (IPA)
- ☐ Information Exchange Agreement (IEA) (if servicing other agencies, e.g., performing fingerprints for Human Resources)

Documents Required for ORI Request to FBI:

1. **Proof that the primary function of the agency is the administration of criminal justice**

Agency Access: Apply for an ORI

ORI – Originating Agency Identifier

- 9-digit Alpha/Numeric Code that serves as an “account” number for your agency.
- Agencies are required to submit documentation to the FBI to prove that the agency is legally authorized access to FBI Criminal Justice Information. The ORI is “proof” of that authorization

Webinars – Criminal Justice Agencies

- How to Apply for a Criminal Justice Agency (CJA) ORI
  - Police, Criminal Courts, Prosecutor, Probation, Corrections

Webinars – Non-Criminal Justice Agencies

- How to Apply for a Non-Criminal Justice Agency (NCJA) ORI
  - Human Resources, Social Services, ICW, CPS, Public Housing, Other agencies with separate HR Department (Day Care, Hospitals, School)
    - First Week of December

User Accounts: Minimum Requirements

TAP TRIBAL ACCESS PROGRAM

Review User Access to Criminal Justice Information (CJI)

- Ensure all users meet the appropriate minimum screening requirements prior to accessing CJI
  - Fingerprint-based record check
  - Training and Certifications
    - CJIS Security Awareness Training (CSAT)
    - NCIC Certification (nexTEST)

CJIS Online

nexTEST CJIS TESTING

Complete User Agency Spreadsheet

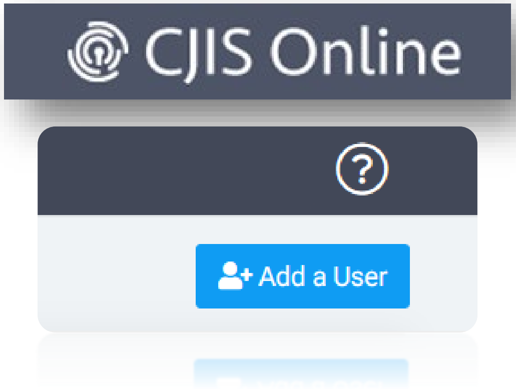
- List all agency employees who have unescorted access to CJI
- Identify staff who will be taking fingerprints
- Identify staff who will be “hands on” operators of JWIN (Name-based)

Notify your TAP BRM of any network, system, or security changes, personnel that will impact their legal authority for access to CJI

Account Management - CSAT

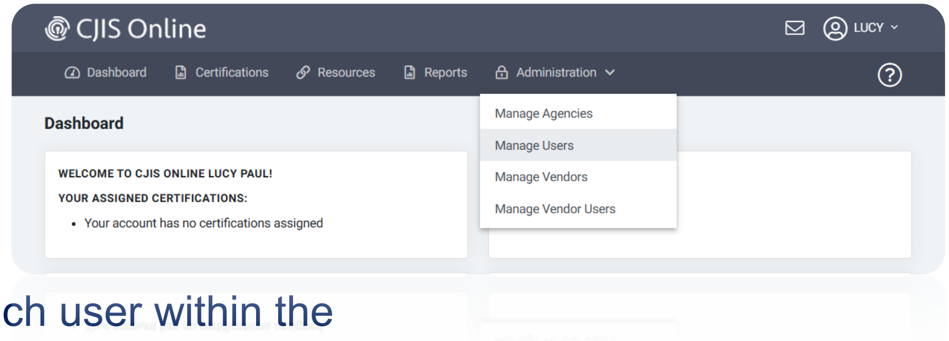
FBI CJIS Security Awareness Training (CSAT)

- Required by all staff who will have unescorted access to FBI provided CJI
- Course is available on-line and consists of a 30 min video and 30 min open-book test.
- Training and Test are on DOJ JCIS Training and Learning Center
  - [Home / JCIS Training and Learning Center (justice.gov)]()
    - *Training account is required to access the test but not the learning page*



Creating and Maintaining Accounts in CJIS Online (link: [CJIS Online]())

- TACs will initiate, maintain, and annually validate CJIS Online user accounts
  - Add Accounts
  - Disable Accounts
  - Validate Accounts
- TACs will be trained in account management
- Ensure training, certification, and user accounts for each user within the agency are current
- Re-certification annually



Dashboard

WELCOME TO CJIS ONLINE LUCY PAUL!

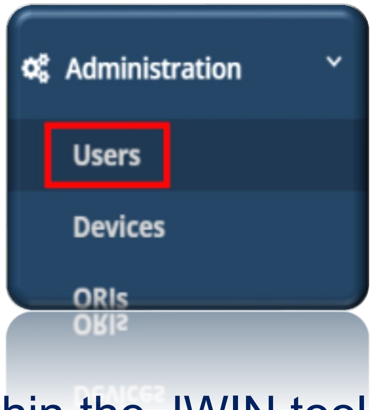
YOUR ASSIGNED CERTIFICATIONS:

- Your account has no certifications assigned

Account Management - JWIN

NCIC Certification Course and Exam

- Ensure completion by all staff who will be “hands on” users of Justice Web Interface to NCIC (JWIN)
- Course is available on-line and consists of 4 videos and open-book test (~ 3 hours total)
- Training and Test are on DOJ JCIS Training and Learning Center
  - Home / JCIS Training and Learning Center (justice.gov)
    - *Training account is required to access the test but not the learning page*



Creating and Maintaining NCIC Certification Accounts

- TACs will create, maintain, and annually validate NCIC accounts within the JWIN tool itself
- TACs will be trained in account management
- Training accounts become “live” accounts after completion of training
- Ensure training, certification, and user accounts for each user within the agency are current
- Re-certification biennially

LEEP and N-DEx Accounts

TRIBAL ACCESS PROGRAM

Law Enforcement Enterprise Portal (LEEP)

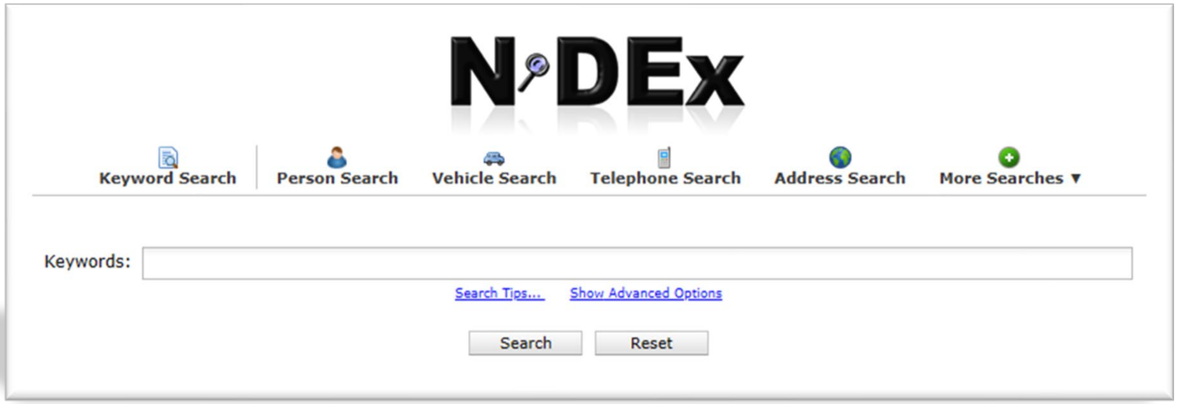
- A LEEP account is required to:
  - Establish an @leo.gov e-mail account
  - Submit fingerprints
  - Exchange CJI between agencies
  - Access N-DEx
- The TAC should ensure that applicable users apply for a LEEP account and monitor the application process
- The TAC must notify the TAP team once accounts are created

LEEP
LAW ENFORCEMENT ENTERPRISE PORTAL

National Data Exchange (N-DEx)

- An online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries
- The TAC assists with establishing access

FEDERAL BUREAU OF INVESTIGATION
@LEO.GOV EMAIL



Post-Deployment Responsibilities

Data Quality of NCIC Records, Users, & ORIs

TRIBAL ACCESS PROGRAM

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
  - Accurate
  - Complete
  - Valid
- 24x7 Hit Confirmation Policy
  - Hit Confirmation Requests

Annual Account and ORI validations

- JABS and CAS (fingerprint) user accounts
- JWIN user accounts
- Agency’s Originating Agency Identifiers (ORIs)

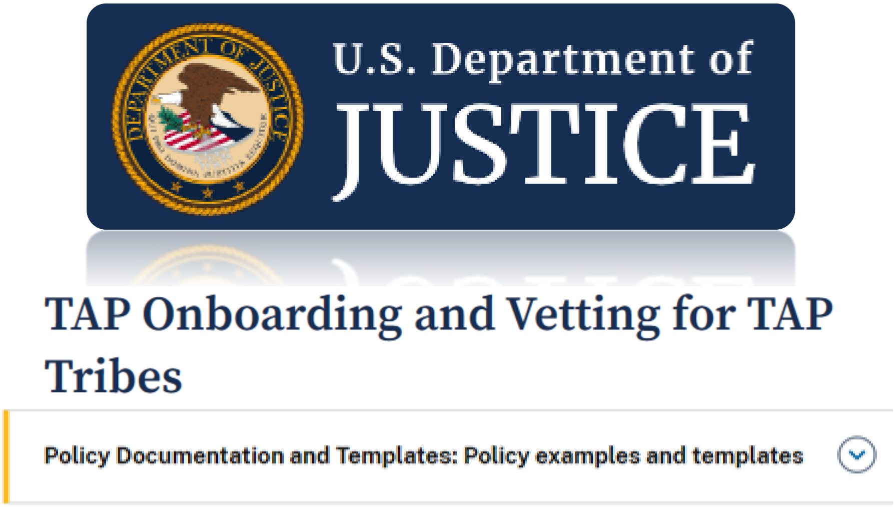
Tribal and Agency Policies related to CJI

The TAC shall ensure agency compliance with FBI CJIS Security Policy

- Agency policies regarding the handling of CJI
- IT Policy – to include:
  - Network segmentation of CJI
  - Incident Response Plan
  - Rules of Behavior
  - Account Management
- DOJ/TAP team has developed policy templates to assist Tribes in developing procedures for all TAP related activities in the Agency

Resources:

- TAP Onboarding and Vetting https://www.justice.gov/tribal/onboarding-and-vetting Password: tribal2019



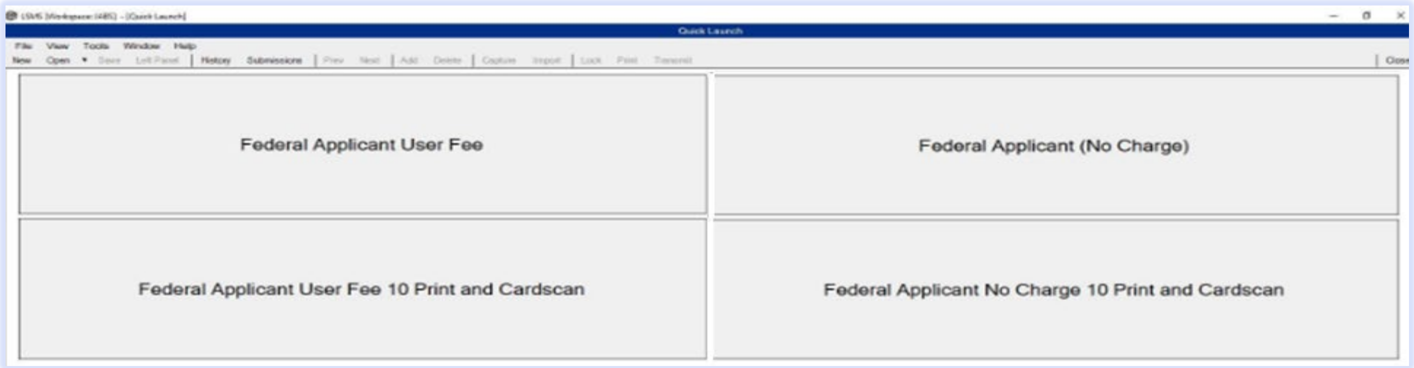
TAP Onboarding and Vetting for TAP Tribes

Policy Documentation and Templates: Policy examples and templates

Fingerprint Submissions

For agencies that submit non-criminal justice agency fingerprints, a TAC must ensure:

- Fingerprinted persons must sign, complete, and return the notice of fingerprint background check and right to challenge form
- Agency uses the correct workflow (FAUF or FANC)
  - Federal Applicant No Charge (FANC) for all Criminal Justice Agency (CJA) Employees
  - Federal Applicant User Fee (FAUF) for all Non-Criminal Justice Agency transactions
- Proper ORI is used for current transaction. E.g. Police may be taking fingerprints on behalf of Social Services. They will have to use the Social Services ORI.
- Understanding of the Reason Fingerprinted field (RFP) and current limitations of fingerprints
- Information Exchange Agreement (IEA) is in place if fingerprinting on behalf of another agency


LSMS [Workspace: (485)] - [Quick Launch]
Quick Launch
File View Tools Window Help
New Open Save Left Panel History Submissions Prev Next Add Delete Capture Import Lock Print Transmit Close
Federal Applicant User Fee
Federal Applicant (No Charge)
Federal Applicant User Fee 10 Print and Cardscan
Federal Applicant No Charge 10 Print and Cardscan

Appropriate Use and Participation in Audits

TACs are responsible for monitoring appropriate use:

- Notify your TAP BRM of any suspected or verified misuse of the national crime information systems
  - When emailing your BRM, always cc: tribalaccess@usdoj.gov
- 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
- 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

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 of requirements

Training and Reference Materials

Training and reference materials:

- TAP Public Website: www.justice.gov/tribal/onboarding-and-vetting | Password: tribal2019
- JCIS Training and Learning Portal: https://csa.justice.gov/jcis/
- CJIS Online: https://www.cjisonline.com/
- DOJ Launch Pad: https://csa.justice.gov/launchpad/
- CJIS Security Policy: https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center
- NCIC Operating Manual: https://csa.justice.gov/cjismanuals/index.pl?cmd=LM&MID=1

Resources

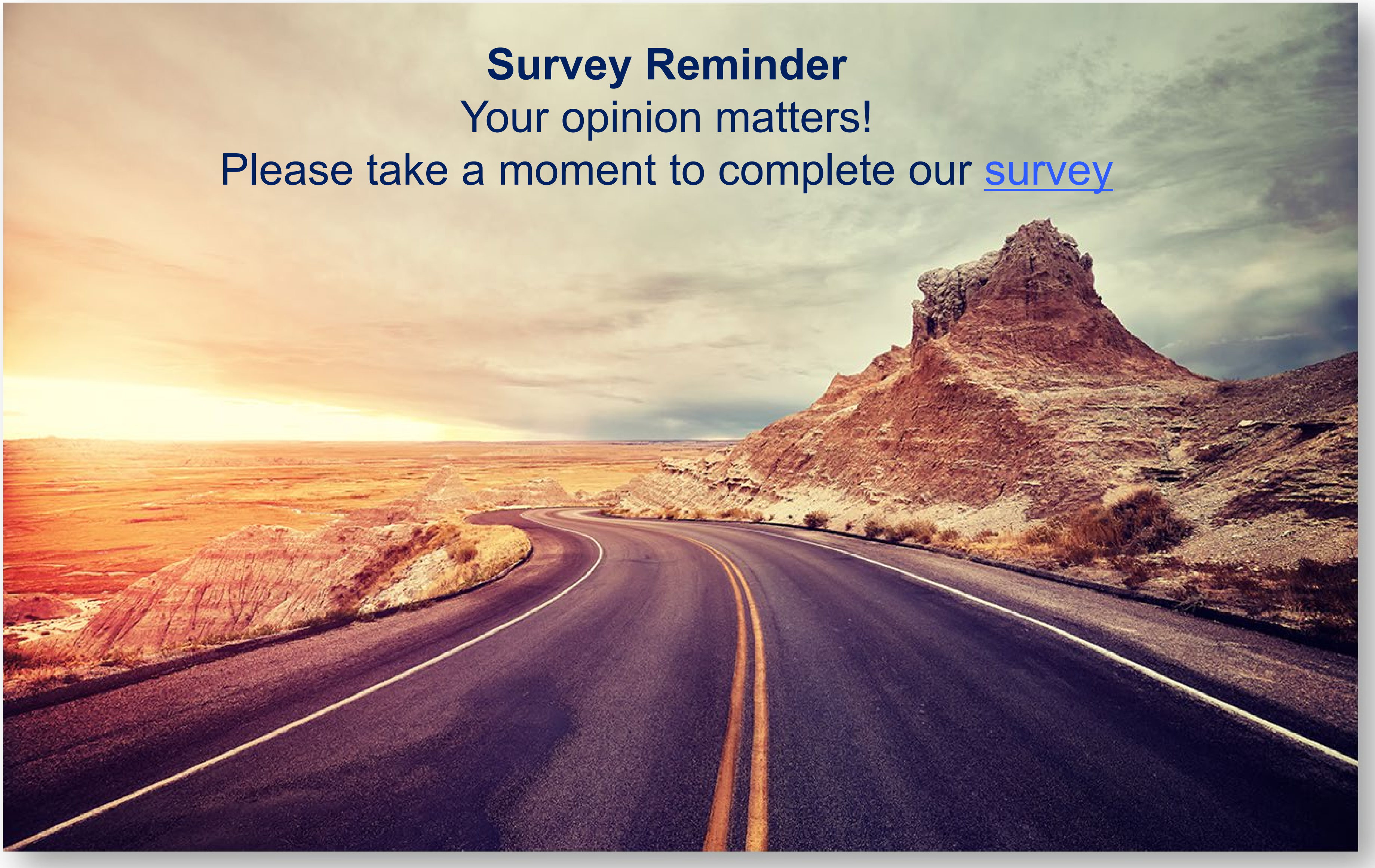
- Contact your Tribe’s assigned Business Relationship Manager (BRM) by email with questions
  - Cc: tribalaccess@usdoj.gov
  - Please include your Tribe’s name in the subject line of the email

- Requests for LEEP technical assistance, account unlocks, and password resets should be directed to the LEEP Support Center
  - LEEP Support Center phone number: (888) 334-4536

- Information on how to order fingerprint cards for the kiosk can be found here: https://forms.fbi.gov/cjis-fingerprinting-supply-requisition-form
  - Order BLANK cards only

- Technical questions and inquiries about the kiosk post deployment should be sent to the HID Support Desk
  - HID Support email: crossmatch.support@hid.com
  - HID Support phone number: (866) 276-7761; Option 1

Questions & Answers



Survey Reminder

Your opinion matters!

Please take a moment to complete our survey