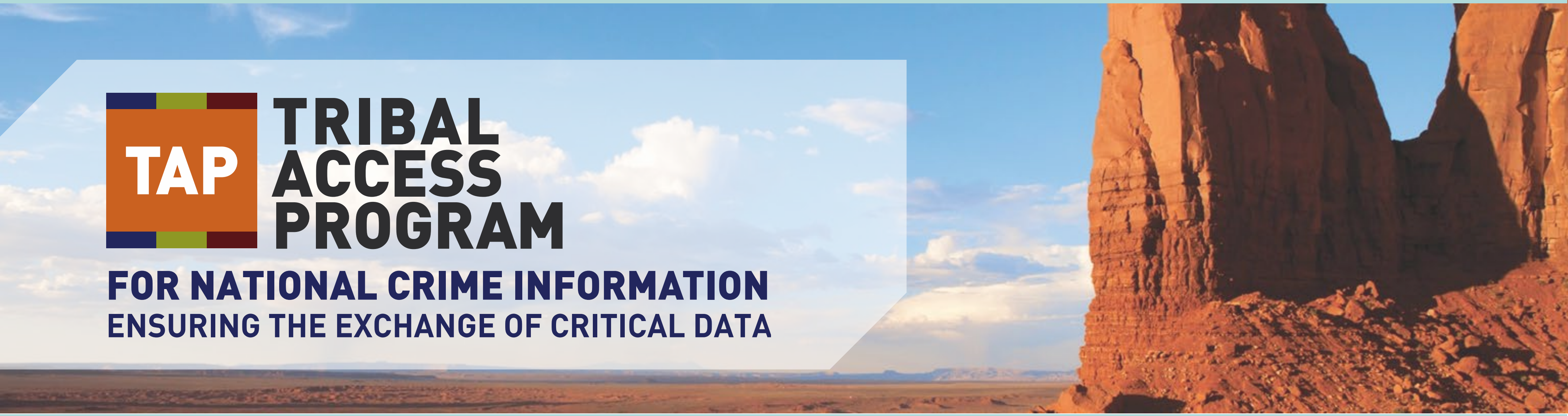

TAP TRIBAL ACCESS PROGRAM

FOR NATIONAL CRIME INFORMATION

ENSURING THE EXCHANGE OF CRITICAL DATA

Audit Overview for TAP Tribal Agencies

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

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

Introduction to Audits: Why are TAP Tribal Agencies Audited?

- All Tribal agencies, including Tribal IT, who participate in the Tribal Access Program (TAP) agreed to be actively engaged and provide documentation to assist in and fully support audits by the Department of Justice (DOJ)
- This audit requirement continues as long as the agency has access and will occur at least once in every three year audit cycle (triennially) per CJIS Security Policy

Introduction to Audits:
Why are TAP Tribal Agencies Audited? (cont'd)

- Per DOJ Justice Criminal Information Services (JCIS) Policy, as the CJIS Systems Agency (CSA) for TAP Tribes, DOJ assumes the responsibility for and enforces system security of all agencies that it services
- In addition to the CJIS Security Policy, this policy establishes the minimum standards for the use of DOJ JCIS systems
  - As the (CSA), DOJ is required to audit every Tribal agency that has access to CJIS systems triennially
  - It is our goal to work in partnership with TAP agencies to educate them about the audit process and ensure they are prepared for a successful audit
  - To that end the DOJ TAP team hosts audit-related webinars for awareness on requirements

Who Participates in an Audit?

- **Tribal Point-of-Contact (POC)**
- **Terminal Agency Coordinator (TAC)**
  - Both must work with DOJ to ensure corrective action is taken if there are audit findings
- Individual users may be required to participate as needed
- Other Tribal personnel with general audit experience
  - May prove helpful to the Tribal agencies participating in DOJ audits

What Programs Areas are Audited?

Audit Area	Agencies Affected	Policy and Procedure Documentation Required
National Crime Information Center (NCIC)	Any agency who accesses NCIC	Yes
National Instant Criminal Background Check System (NICS)	Law Enforcement, Criminal and Civil Courts, Probation, Prosecutor's Office	Yes
National Data Exchange (N-DEx)	Any criminal justice agency	No
National Sex Offender Registry (NSOR)	Agency who submits the NCIC/NSOR record; usually Law Enforcement	Yes
National Identity Services (NIS) (Civil Fingerprints)	Social Services, Human Resources, Housing and CJAs for employment purposes	Yes
Information Technology (IT)	IT	Yes

Examples of Topics Covered During an Audit

- All systems are auditable and can cover the following areas:
  - Use of correct ORI for transactions
  - Documentation to support entries
  - Data quality
  - Background screening of individuals with access to Criminal Justice Information
  - Use, access and dissemination of criminal history record information (CHRI)
  - Timeliness of entries
  - User training certifications
  - IT security
  - Other topics as needed

DOJ Audit Process – Online vs On-site

Online Audit

- Online audits are conducted through questionnaires that are accessed through the JCIS Audit portal
- Each Tribal agency questionnaire will cover only the program areas the Tribal agency utilizes
- JCIS Audit tutorials are available to assist in filling out the questionnaires
- The audit process can be temporarily suspended and finished during a later session if the user requires the interruption

On-Site Audit

- Tribal agencies will be randomly selected for an on-site audit which will be scheduled by the DOJ audit team.
- Provides 4-6 weeks notice to the TAC to schedule the onsite audit; letter providing formal notification to follow
- Works closely with the TAC to provide pre-audit materials such as questionnaires, surveys, list of records to be reviewed
- Interviews TAC and other agency, personnel, reviews documentation and provides verbal recommendations on audit day
- Provides a written report within 2 weeks of the audit documenting the audit recommendations
- Reviews Tribal agency’s written corrective action plan

DOJ Audit Resources

- DOJ JCIS Training and Learning Center https://nextest.just.jmd.usdoj.gov/cjin/index.php
  - CJIS Manuals
  - CJIS Security Policy v5.7
  - Terminal Agency Coordinator (TAC) & User Resources

DOJ TAP - CJIS Audit Support

- TAP team support and engagement continues beyond today's training
- Contact the Tribe's assigned Business Relationship Manager and cc: tribalaccess@usdoj.gov; please include the Tribe's name in the subject line of the email
- TAP team will host topic-specific audit webinars
  - IT
  - NSOR
  - NICS
  - N-DEx
  - NCIC
  - NIS (civil fingerprint)

Resources

- Training and reference materials can be found in the JCIS 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