TRIBAL CONSULTATION FRAMING PAPER:
Implementing Compliance Audits of Tribal User Agencies With Access To FBI CJIS Systems and Information via TAP

December 2019

Law Enforcement Services & Information Sharing
Office of the Chief Information Officer
United States Department of Justice
Two Constitution Square (2CON)
145 N Street NE
Washington, DC 20002

Tribal Access Program: In 2015, DOJ established the Tribal Access Program for National Crime Information (TAP), which provides federally-recognized Tribes access to national criminal justice information systems for authorized criminal and non-criminal justice purposes to more effectively serve and protect their nation's citizens. TAP User Agencies include law enforcement, jails, prosecutors, courts, probation and pretrial services, as well as non-criminal justice agencies for specifically authorized non-criminal justice purposes, such as screening for child placement, housing, sex offender registration, and civil court entry of orders of protection.

FBI CJIS databases: The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) maintains the central repository for criminal justice information services, and provides a telecommunication network to CJIS Systems Agencies (CSAs) in each of the 50 states, the District of Columbia, U.S. Territories, Canada, and various federal agencies, including DOJ. CSAs provide access the the national crimal justice information systems, and are responsible to ensure that their User Agencies and individual system users are familiar with and comply with all applicable laws, regulations, and related requirements that govern the use of the information systems. TAP User Agencies utilize the DOJ as their CSA.

FBI CJIS audit requirements: FBI CJIS Security Policy has two audit requirements that will affect Tribal User Agencies in TAP:

- First, the Policy requires that each CSA, including DOJ, audit each of their User Agencies, including Tribal User Agencies, at least once every three years. DOJ is required to perform the audit to verify User Agency and individual user compliance with applicable laws, regulations, and polices, as they pertain to the use of access to Criminal Justice Information (CJI) and Criminal History Record Information (CHRI) through its network.
    - There is no cost to any User Agency, including TAP User Agencies, for the audit.
- Second, to ensure that its CSAs are performing audits as required by the Policy, FBI CJIS audits all of its CSAs, including DOJ, as well as a small number of selected User Agencies at least once every three years. As part of that second type of audit, Tribal User Agencies may be selected for an audit by FBI CJIS.

DOJ CSA User Agency: A User Agency is the entity legally authorized by FBI CJIS to submit or receive information from FBI CJIS Systems, either as a Criminal Justice Agency (CJA) or a Non-Criminal Justice Agency (NCJA). Typical CJAs are a law enforcement agency, a jail or a probation department. Typical NCJAs are a sex offender registry agency, a civil court or a housing authority. Every Tribe will thus have a number of User Agencies, both CJA and NCJA, each of which must be audited at least once every three years.

DOJ's Audit Policy: DOJ is updating its required audit policy, so that it is both more efficient and more effective, but does not unnecessarily burden User Agency personnel. Currently, DOJ is piloting an interim audit policy with non-Tribal User Agencies; that interim policy is set forth at the end of this framing paper for review. Briefly, it utilizes the following methodology:

- Online Phase:
  - All User Agencies participate in the Online Phase
  - User Agencies receive online questionaires to be completed
  - The number of questionaires depends on the data and services the User Agency accesses
  - User Agencies provide documents in support of answers via encrypted email or secure file transfer mechanism
  - An online audit tool is available which provides tutorials to assist User Agencies in completing the online questionaires
- Onsite Verification Phase:
  - Selected User Agencies and selected agency field units are chosen for an Onsite Verification of their questionaires
  - DOJ's auditor makes an onsite visit to meeting with various User Agency personnel, confirms the online questionnaire responses, and collects additional material during the visit if needed

DOJ is seeking input from Tribes on the audit methodology. DOJ believes any audit program should:

- Lower User Agency risk of inappropriate system/information use and handling
- Assist User Agencies in identifying best use practices
- Advise User Agencies in improving activities to ensure they are efficient and cost effective

Tribal Consultation Questions:

- The TAP team that currently works with Tribes in the program could collect documents that would be useful in an audit, including policies, training logs, consent forms, etc. Would it be acceptable for OCIO to access those documents from the TAP team for audit purposes? If so, what notification would you like (i.e. an email notification to let you know when the auditors intend to access your documents)?

- Non-Tribal user agencies are audited at random every three years, but given the number of user agencies within each Tribe, we believe it would be more helpful and less burdensome to audit all of a Tribe's user agencies at one time. Would this be acceptable?

- In the interim policy that non-Tribal agencies are currently piloting, all agencies being audited must complete an online audit and an additional percentage must also undergo an on-site verification of the online audit answers. The attached sample audit questionnaire will give you an idea of the scope and depth of the audit. We would like to understand the implications of periodically doing both an online audit and an onsite verification for your operations. For example, what adjustments to your normal operations would you have to make to complete both?

- We welcome your feedback on the criteria used to select User Agencies for on-site verification. Under the interim policy, some User Agencies are selected for Onsite Verification at random but some are selected based on a combination of factors, which include risk (e.g. poor historical compliance, new User Agency status, unique system-use cases, etc.), as well as complex User Agency structure (e.g. geographical distribution, size, structure, function, etc.). Do you agree with these risk factors? Would you change or add to this criteria?

- TAP currently provides audit preparation webinars. Would additional support in advance of an audit be helpful (i.e. additional training)? If so, what additional support would be helpful?

- We welcome your input on any redundancies or inefficiencies in the processes described here and in the attachments. One of our goals is to ensure we are doing everything possible on our end to reduce the administrative burden and disruption associated with being audited.