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

Tribal Access Program (TAP) for National Crime Information

User Feedback Phase: Final Report v1.0

December 19, 2016

Table of Contents

Executive Summary

While the Violence Against Women Act of 2005 (VAWA) and the Tribal Law and Order Act of 2010 (TLOA) require the Attorney General to ensure that tribal law enforcement officials who meet applicable federal or state requirements be permitted access to national crime information databases, the reality is that the ability of tribes to fully participate in national criminal justice information sharing via state networks depends upon various regulations, statutes, and policies of the states in which a tribe's land is located. As a result, the Department of Justice (DOJ) repeatedly has heard from tribes that they face barriers to accessing and entering information into national crime information databases.

In August 2015, DOJ initiated the Tribal Access Program for National Crime Information (TAP) and by November 2015, nine tribes had been selected for participation. The DOJ Office of the Chief Information Officer (OCIO) operates TAP, but in reality, it is a collaboration between OCIO, DOJ Office of Tribal Justice (OTJ), DOJ's Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART), FBI's Criminal Justice Information Systems Division (CJIS), DOJ's Community Oriented Policing Services (COPS) and the tribes themselves. TAP consists of three primary elements:access, technology, and training. Access to national crime information databases is provided via the OCIO which acts as the CJIS Systems Agency (CSA) for tribes unable or unwilling to access CJIS-managed services through state networks. Tribes participating in TAP receive an integrated workstation that includes a computer, fingerprint/palmprint scanner, integrated camera (for mugshots and photographs of scars, marks and tattoos); flatbed scanner (for capture of inked fingerprint cards); a printer; and an optional ruggedized kiosk cabinet. The three software applications on the workstation provide access to over half a dozen criminal information databases including the National Crime Information Center (NCIC); FBI's fingerprint and biometric system, Next Generation Identification (NGI); the national repository of criminal histories, the Interstate Identification Index (III); and the International Justice and Public Safety Network (Nlets). TAP also provides tribes a full day of on-site training as well as access to an online Training and Learning portal containing training videos, job aids, fact sheets, and certification tests for CJIS Awareness Training and NCIC usage.

DOJ is implementing TAP in phases. The FY16 deployment was the "User Feedback Phase."Funded entirely by SMART, this phase was used to evaluate the onboarding and vetting process, technology, training and support, and information gaps, as well as to provide an opportunity for tribes to share lessons learned and best practices.By the end of August 2016, the TAP team completed deployment to the nine User Feedback Phase tribes and began collecting quantitative usage metrics as well as qualitative feedback of the process.During the User Feedback Phase, the major challenges were in the following areas:

Whole of Government Decisions - For many tribes, participation in the TAP program was the first time many non-law enforcement criminal justice agencies and civil agencies had direct access to national crime information databases. Cross-agency decisions were required that affected all tribal agencies and questions about how they would work together to make the most effective use of the TAP resources arose. Some of the major decisions included:

- What criminal data will the tribe enter into national crime information databases? Does the tribe have the resources to support the responsibilities that are required when information is entered?
- Which agencies will actually submit transactions and which agencies may have transactions submitted on their behalf by another agency? How will Criminal Justice Information (CJI) be transmitted and protected as required?
- Where will the workstation be physically located, especially if multiple agencies plan to access it?

Limitations with Federal Legal Authorities for Civil Background Checks - Under TAP, the participating tribes access national crime information databases as federal users, and thus were required to utilize more limited federal legal authority, rather than state authority. States have much more broad authority to authorize civil background checks. The TAP team worked closely with FBI CJIS Office of General Council (OGC) to identify the appropriate federal legal authorities under which tribal civil agencies such as social services, public housing, and child protective services could access national crime information databases for the purpose of conducting background checks.

Onboarding and Vetting (OB&V) Challenges – Both TAP and the tribes experienced challenges during the onboarding and vetting process. The TAP team did not have an OB&V infrastructure or well-defined procedures and documents in place when TAP began. Thus, the TAP team developed "Vetting Packages" which contained documentation; Reimbursable Agreement templates; and checklists to include required documentation lists for Criminal Justice Agencies (CJA), Non-Law Enforcement CJAs, and Non-CJAs needed to receive access authority from FBI CJIS. The TAP team also developed "Onboarding Packages" to ensure all pre-deployment activities were completed. These consisted of documentation that included a CJIN Workstation Configuration form; IT Review Checklists; Checklists for a Physically Secure location; Technical Specifications for OFM on a PC; User Account Spreadsheet; Templates for Background Investigation Policy, User Agency Agreement (UAA) and TAP Addendum; and templates for Interagency Agreements. In addition, the TAP team developed, recorded and posted the online training modules, job aid, fact sheets, and CJIS Security Awareness Training and Certification and the NCIC Training and Certification required for access to Criminal Justice information and access to NCIC.

One of the most immediate challenges during the OB&V period was the length of time it took tribes to complete the required tasks. Initially the TAP team approached the OB&V process at the tribal level and planned to process nine tribes, estimating that no more than 30 days would be required for each. However, in reality, each tribal agency had to undergo separate vetting and partially separate onboarding. This increased the real workload from nine tribes to sixty-five agencies. In addition, some tribal agencies required additional time to complete the OB&V process. Reasons for this varied but included:

- Difficulty collecting the required documentation for submission when applying for an originating agency identifier (ORI), a nine-digit code used by agencies on the criminal justice network
- Difficulty collecting the signed documents such as UAAs, TAP Addendums, and Information Exchange Agreements (IEA)
- The fact that each agency was undergoing OB&V separately meant that the tribe as a whole generally could not move forward until the majority of agencies received ORIs (we did in some cases move forward, while still waiting for ORIs for some agencies)
- Civil agencies took longer to vet because Reimbursable Agreements for payment of civil fingerprint-based background check fees had to be put in place between the tribes and CJIS. This process took anywhere from four to sixteen weeks
- Meeting requirements for physical security (e.g. secure, locked area) for the TAP workstation; several tribes had to specially install and configure internet connections and/or prepare secure areas for the TAP workstation
- Technical issues related to the tribe's IT staff providing the public facing IP address led to delays in personnel from the tribe being able to access the online training/certification. There were further issuing in identifying and collecting the required information to create training/user accounts for all the users resulting in delays with personnel actually completing the training in a timely manner. All individuals attending deployment day training were required to, at a minimum, complete the CJIS Security Awareness Training
- Working through some of the whole of government decisions which required careful consideration of which agencies would be participating, how they would share information, and the location of the workstation
- Having a tribal POC that was not at the executive level and thus could not enforce actions or milestones from agency heads, when needed

Process improvements from these challenges and lessons learned are being incorporated into the FY17 Phase of TAP. The TAP team now has a robust OB&V process with templates, better understanding of the technical challenges on site, several well understood interagency cooperation models, a good understanding of current federal legal authorities and their boundaries, and 9 deployed tribes who are available for advice and support to make FY17 a very good year for TAP.

1 Background

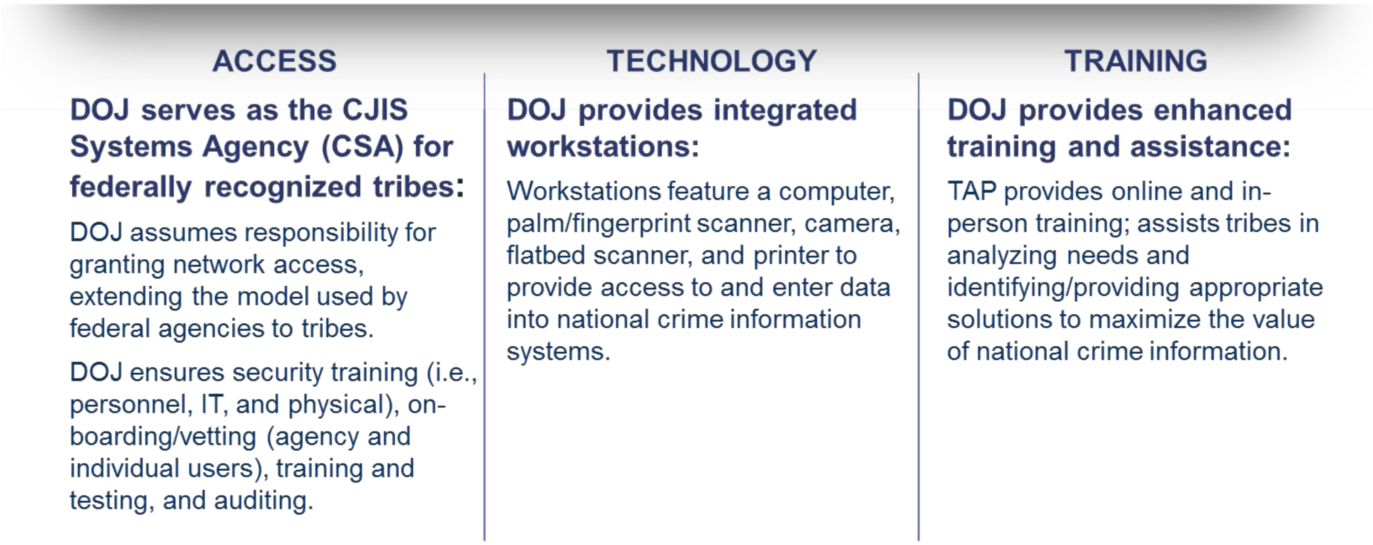
While the Violence Against Women Act of 2005 (VAWA) and the Tribal Law and Order Act of 2010 (TLOA) require the Attorney General to ensure that tribal law enforcement officials who meet applicable federal or state requirements be permitted access to national crime information databases, the reality is that the ability of tribes to fully participate in national criminal justice information sharing via state networks depends upon various regulations, statutes, and policies of the states in which a tribe's land is located. As a result, DOJ has repeatedly heard from tribes that they face barriers to accessing and entering information into national crime information databases.

The lack of access to criminal databases also results in tribal records being unavailable to other jurisdictions; e.g., minimal information regarding suspects and no access to tribal fingerprints, bookings, or information about the arrest dispositions. Moreover, tribes may be unable to access criminal records about non-Indians and non-member Indians committing offenses on their reservation. Such an information vacuum puts responding officers, victims, and the community in jeopardy.

Tribal governmental agencies also need access to criminal history record information for non-criminal justice employment and licensing purposes. Statutory authority for access largely depends on the purposes and may vary tribe-to-tribe. Commonly authorized purposes include screening for: tribal government personnel, social workers, medical, and school personnel, tribal housing authority employees and prospective tenants, foster care placement, or for personnel working with children. Specific legislation or provisions within broader statutes, such as the Indian Child Protection & Family Violence Prevention Act, and Native American Housing Assistance and Self-Determination Act, authorize or, in some instances, require background checks to be completed.

2 Overview of the Tribal Access Program for National Crime Information (TAP)

In August 2015, DOJ initiated the Tribal Access Program for National Crime Information (TAP). TAP is operated by the DOJ Office of the Chief Information Officer (OCIO), but in reality, it is a collaboration between OCIO, DOJ's Office of Tribal Justice (OTJ), DOJ's Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART), FBI's Criminal Justice Information Systems Division (CJIS), DOJ's Community Oriented Policing Services (COPS) and the tribes themselves. TAP consists of three primary elements: access, technology, and training; these are summarized in the following sections (Figure 1).



ACCESS

DOJ serves as the CJIS Systems Agency (CSA) for federally recognized tribes:

DOJ assumes responsibility for granting network access, extending the model used by federal agencies to tribes.

DOJ ensures security training (i.e., personnel, IT, and physical), on-boarding/vetting (agency and individual users), training and testing, and auditing.

TECHNOLOGY

DOJ provides integrated workstations:

Workstations feature a computer, palm/fingerprint scanner, camera, flatbed scanner, and printer to provide access to and enter data into national crime information systems.

TRAINING

DOJ provides enhanced training and assistance:

TAP provides online and in-person training; assists tribes in analyzing needs and identifying/providing appropriate solutions to maximize the value of national crime information.

Figure 1: Three Elements of TAP

2.1 Access

Prior to TAP, tribal access to national criminal databases was only available through the state CJIS Systems Agency (CSA) via the state switch. This access was accompanied by constraints, limitations, or conditions that may not have taken into account tribal sovereignty. In some cases, tribes felt that as sovereign nations, they should not be required to rely on states or local authorities to enter data on their behalf. In other cases, tribes had no access as their law enforcement agencies were not seen as legitimate in the states in which their land is located. Finally, sometimes tribes had limited query access, but not entry capabilities.

Under TAP, the OCIO acts as the CJIS Systems Agency (CSA) for participating tribes. Thus, OCIO assumes responsibility for granting network access to tribes using the same model used by federal agencies accessing national crime information databases through DOJ. This access eliminates potential constraints and provides participating tribes with the same level of access to national criminal information databases as any other federal agency.

In some cases, data available from national crime information databases may not necessarily represent all information available from in-state agencies, as states chose what information they want to submit to the entirely-voluntary national databases. Thus, there may be instances when the use of DOJ as the CSA could result in less information being available than if the tribe had accessed those databases through their state CSA. DOJ recognizes that in many instances, tribes receive additional benefits from participating in state law enforcement networks and access to national criminal databases through their state CSA. DOJ strongly discourages tribes from abandoning productive relationships with states.

2.1.1 Access to National Crime Information Databases

Through TAP, participating tribes have access to the following National crime information databases:

- ***National Crime Information Center (NCIC)*** – a criminal records database allowing criminal justice agencies to enter or search for information about stolen property, missing or wanted persons, and orders of protection; and to access the National Sex Offender Registry
- ***Next Generation Identification (NGI)*** – a database of palm, fingerprints, and mugshots, allowing verification of identity, submissions of arrest information, and access to fingerprint-based criminal histories
- ***Interstate Identification Index (III)*** – provides for the decentralized interstate exchange of criminal history record information. III functions in conjunction with the CJIS Next Generation Identification system, or NGI
- ***National Data Exchange (N-DEx)*** – a national investigative information sharing system giving access to records from across the nation to aid in criminal investigations
- ***National Instant Criminal Background Check System (NICS) –*** a system used by Federal Firearms Licensees (FFLs) to determine a person's eligibility to buy firearms or explosives. Used by law enforcement agencies to dispose of firearms and to issue weapons permits
- ***Law Enforcement Enterprise Portal (LEEP) –*** a gateway for criminal justice agencies to access unclassified law enforcement intelligence products and systems. Also used for encrypted secure email communications with NGI
- ***International Justice and Public Safety Network (Nlets)*** – an interstate justice and public safety network owned by the states supporting inquiry into state systems for criminal history driver's license and motor vehicle registration, as well as supporting inquiry into federal systems

Various federal legal authorities limit each tribal agency to specific data sources for specific purposes. With the exception of Criminal Justice Agencies, all other agencies have limitations.

2.2 Technology

TAP provides participating tribes with an integrated workstation at no cost. It consists of:

- ***Computer/monitor*** – containing the TAP applications (described below)
- ***Fingerprint /palm print scanner*** – for electronic capture of finger and palm prints of sufficient quality for acceptance by FBI's NGI
- ***Integrated camera*** - for facial photographs (mug shots) and photographs of scars, marks, and tattoos
- ***Flatbed scanner*** – for scanning inked fingerprint cards
- ***Printer*** – capable of printing both criminal and civil finger and palm print cards

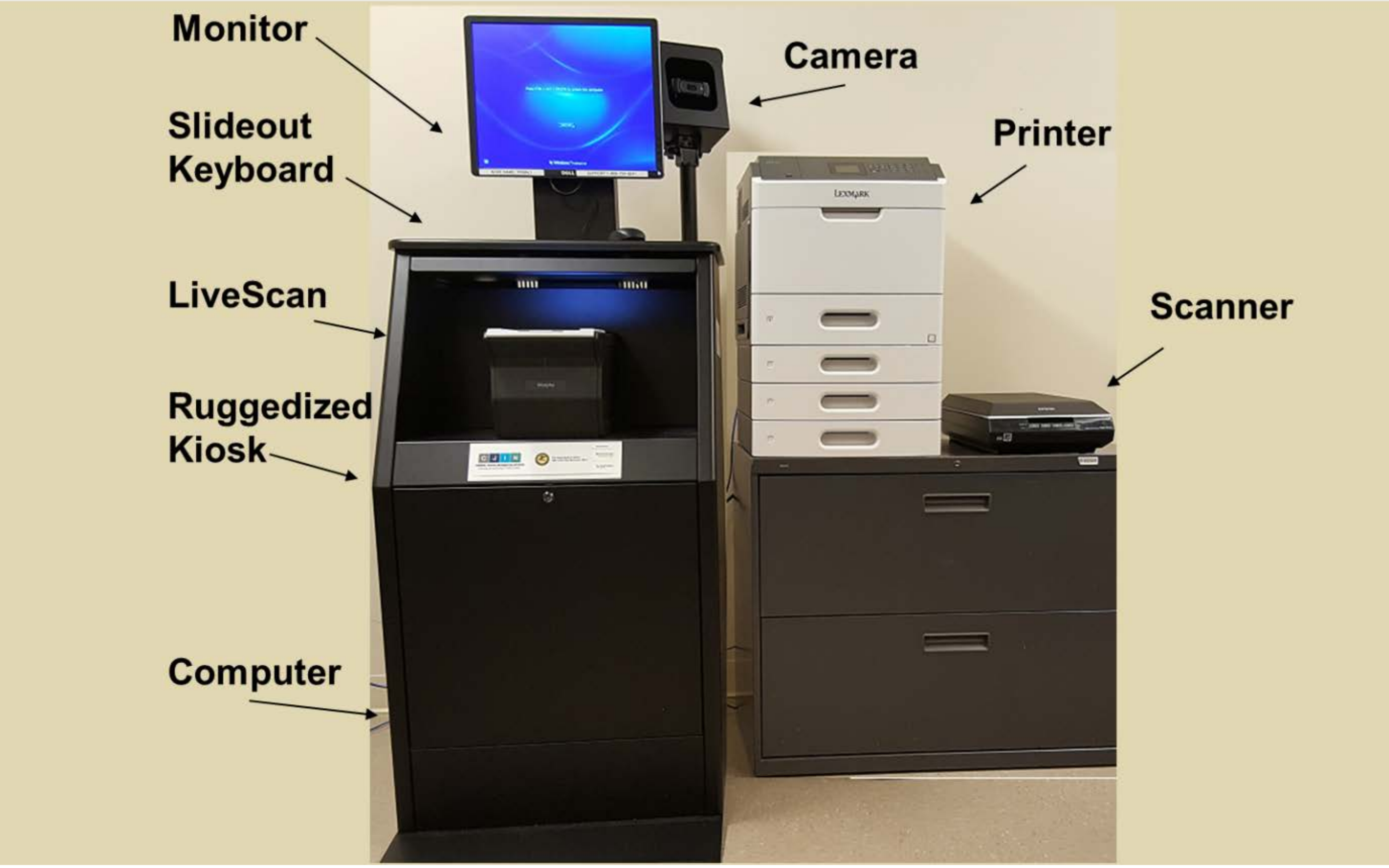


Figure 2: TAP Workstation

The workstation is simple to use and contains three applications that provide access to over a half dozen criminal information databases (Figure 3)

- ***MESA*** – used to create fingerprint-based arrest bookings, identification, and sex offender registrations. Also used to conduct fingerprint-based background checks
- ***OpenFox Messenger*** – provides access to name-based checks through NCIC, III, and Nlets
- ***LEEP via Internet Explorer*** – provides access to allow secure, encrypted email used in transmitting files to NGI and portal access to dozens of unclassified law enforcement databases

The TAP workstation is available in four configurations depending on tribal needs.

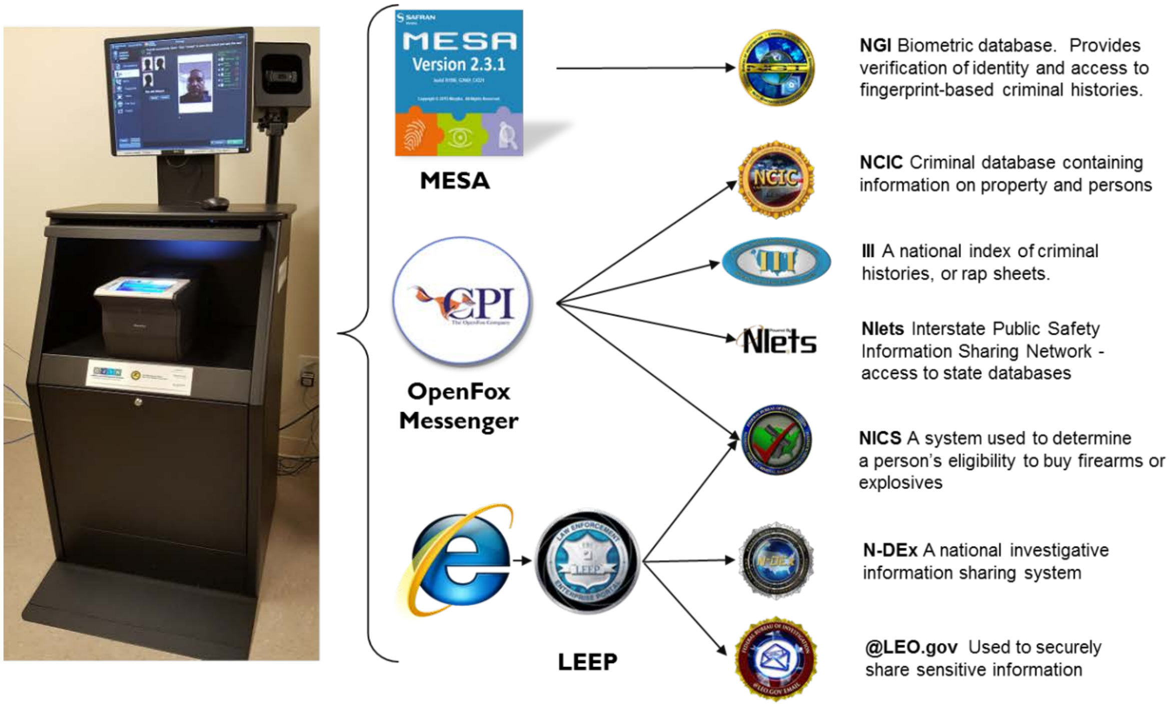

MESA
Version 2.3.1
MESA
OpenFox Messenger
LEEP
NGI Biometric database. Provides verification of identity and access to fingerprint-based criminal histories.
NCIC Criminal database containing information on property and persons
III A national index of criminal histories, or rap sheets.
Nlets Interstate Public Safety Information Sharing Network - access to state databases
NICS A system used to determine a person's eligibility to buy firearms or explosives
N-DEx A national investigative information sharing system
@LEO.gov Used to securely share sensitive information

Figure 3: TAP Workstation Software

Maintenance and support for the workstation is provided by DOJ through the vendor's Customer Care Center (CSC). The CSC staff are available 24/7 for any issues related to the workstation, hardware peripherals, or any of the workstation software.

2.3 Training and Support

DOJ provides enhanced training and assistance that includes in-person training at the tribe during the initial deployment, as well as web-based learning resources available before and after deployment.

In addition, the TAP team assists tribes in looking at "whole of government" decisions to maximize the use of TAP. Tribes are asked to evaluate the needs of all agencies that will use TAP and make decisions to ensure that TAP services are easily accessible to all participating agencies within the tribe, and are used in the most efficient way within the tribal government.

2.3.1 Required Training - Prior to deployment

The following training and certification requirements are necessary prior to deployment and prior to accessing the OpenFox Messenger application. These courses and their corresponding certifications tests are available on the on-line training portal:

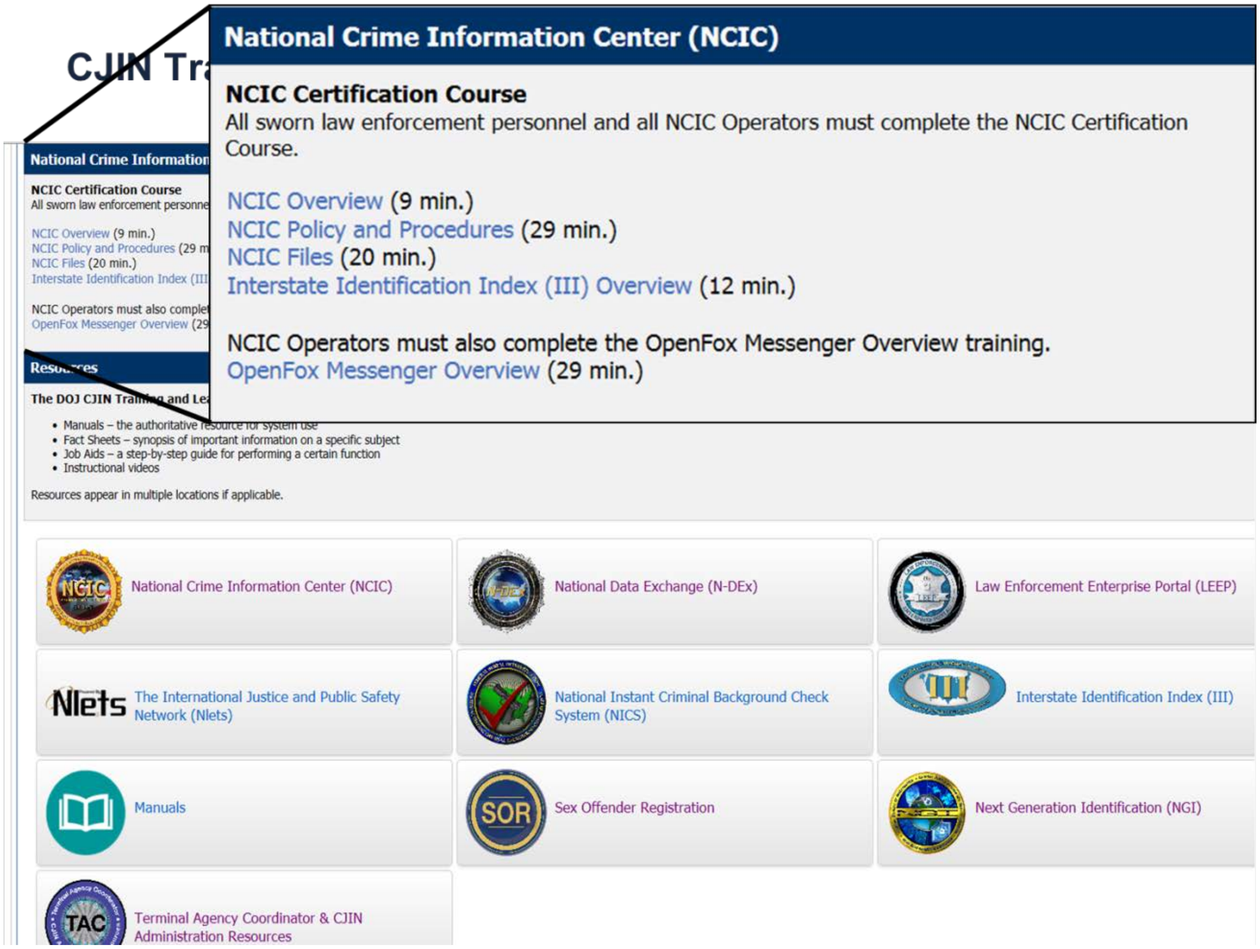
- All users must complete CJIS Security Awareness Training (CSAT) and certification test
- All sworn law enforcement personnel and all NCIC Operators must complete the NCIC Certification Course and test
- All NCIC Operators must complete the NCIC Certification test
- All users who are submitting fingerprints to CJIS must register for a LEEP account

2.3.2 CJIN Training and Learning Portal

The CJIN Training and Learning Portal was developed especially for TAP (Figure 4). Prior to its development, customers were required to travel to DOJ in Washington, DC to complete NCIC training and take the certification test. There were no simple training resources to educate users about the national crime databases, how to best utilize them, and the relationships/interdependencies between them.

The CJIN Training and Learning Portal contains various types of materials:

- ***Training Videos*** – five to thirty minute videos providing introductory material to CJIS systems, e.g. "Usage of OpenFox Messenger Operation," "How to Conduct a Sex Offender Registration," and more
- ***Job Aids*** – Brief "How To" guides that walk a user through a specific task, e.g. "How to register for a LEEP Account" or "How to submit a booking to NGI"
- ***Fact Sheets*** – Brief informational papers on various topics related to TAP, e.g. "Requirements for 24/7 Hit Confirmation Monitoring"
- ***Training and Certifications*** – Training and Certification tests are available on-line for both CJIS Security and Awareness Training (CSAT) and NCIC access. These certifications are linked to OpenFox Messenger accounts so that the accounts cannot be activated until the required certification tests has been completed



CJIN Tr

National Crime Information Center (NCIC)

NCIC Certification Course
All sworn law enforcement personnel and all NCIC Operators must complete the NCIC Certification Course.

NCIC Overview (9 min.)
NCIC Policy and Procedures (29 min.)
NCIC Files (20 min.)
Interstate Identification Index (III) Overview (12 min.)

NCIC Operators must also complete the OpenFox Messenger Overview training.
OpenFox Messenger Overview (29 min.)

Resources

The DOJ CJIN Training and Le

- Manuals – the authoritative resource for system use
- Fact Sheets – synopsis of important information on a specific subject
- Job Aids – a step-by-step guide for performing a certain function
- Instructional videos

Resources appear in multiple locations if applicable.

National Crime Information Center (NCIC)
National Data Exchange (N-DEx)
Law Enforcement Enterprise Portal (LEEP)
Nlets The International Justice and Public Safety Network (Nlets)
National Instant Criminal Background Check System (NICS)
Interstate Identification Index (III)
Manuals
SOR Sex Offender Registration
Next Generation Identification (NGI)
TAC Terminal Agency Coordinator & CJIN Administration Resources

Figure 4: CJIN Training and Learning Portal

3 User Feedback Phase

TAP is being implemented in phases. The first phase, the User Feedback Phase, was funded by the SMART Office and was used to evaluate DOJ's technology solution; evaluate information gaps between federal and state sources; evaluate training and support needs; and identify and share best practices regarding use. The basics steps of the User Feedback Phase include the following, each of which is described in further detail below (see Figure 5):

- Application and Selection
- Onboarding and Vetting
- Deployment
- User Feedback and Evaluation

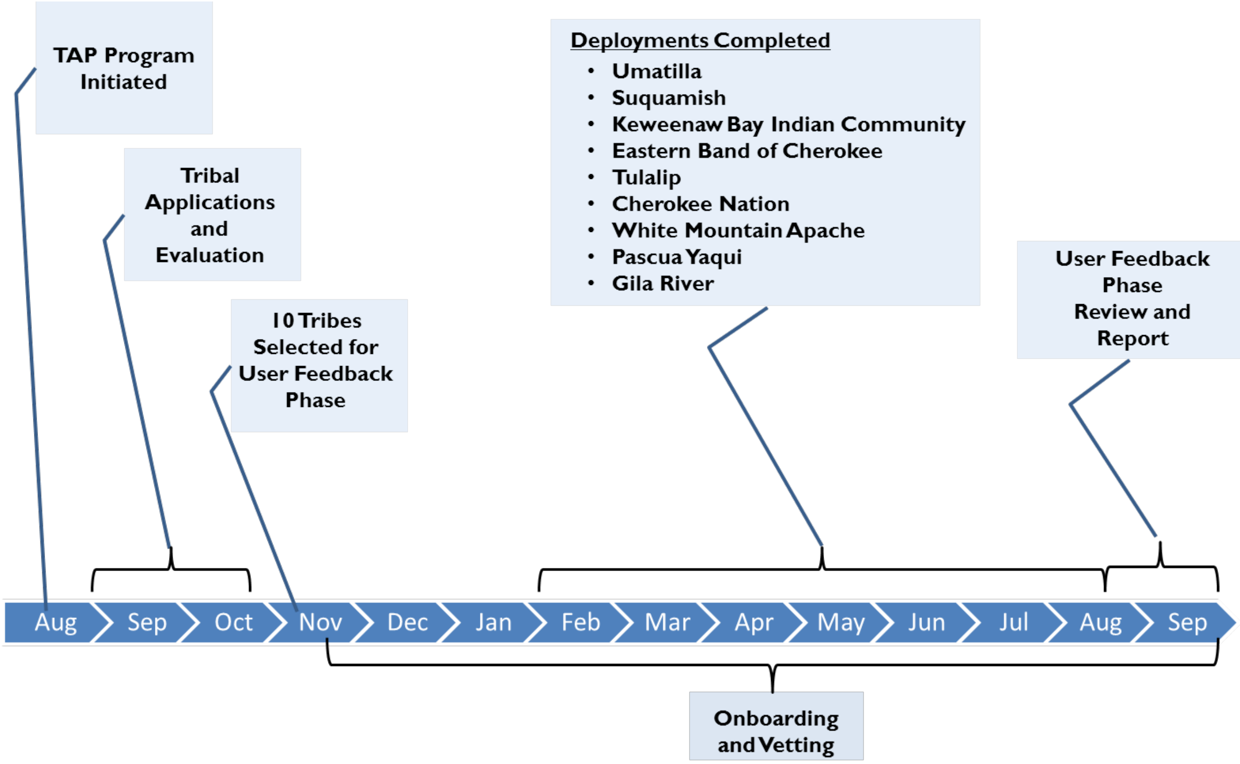


Figure 5: TAP User Feedback Phase Schedule

3.1 Applicants and Selection

Following the announcement of TAP in August 2015, interested tribes submitted "Letters of Interest." To be considered for TAP, the applicant tribes had to:

- be a SORNA tribe with the responsibility of running an Adam Walsh Sex Offender registry;
- have a law enforcement agency with arrest powers;
- have a well-defined civil/noncriminal justice need (i.e. child placement, housing, etc.); and
- not be a BIA direct-service law enforcement tribe

Tribes agreed to comply with the CJIS security policies, CJIS system policies, and all DOJ CSA policies. Tribes were also responsible for providing high-speed internet access (DSL speed or higher) and paying FBI CJIS User Fees associated with fingerprint-based background checks for noncriminal justice purposes. Thus, participating tribes had to execute a user fee memorandum of understanding (MOU) with CJIS to pay those fees. On November 11, 2016, DOJ announced the 10 tribes selected; they included:

1. Cherokee Nation
2. Confederated Tribes of the Umatilla Indian Reservation
3. Eastern Band of Cherokee Indians
4. Keweenaw Bay Indian Community, Michigan
5. Oneida Nation of New York
6. Pascua Yaqui Tribe of Arizona

7. Shoshone-Bannock Tribes of the Fort Hall Reservation
8. Suquamish Indian Tribe of the Port Madison Reservation
9. Tulalip Tribes of Washington
10. White Mountain Apache Tribe of the Fort Apache Reservation, Arizona

During the process, two tribes chose to terminate their participation in TAP (Oneida and Shoshone-Bannock) and one new tribe, Gila River Indian Community of the Gila River Indian Reservation, Arizona was added, for a total of nine tribes participating in the User Feedback Phase.

3.2 Onboarding and Vetting (OB&V)

Once the tribes were selected, the Onboarding and Vetting (OB&V) process began. Each tribe was assigned a Business Relationship Manager (BRM) to serve as the TAP team point of contact for the tribe and to assist the tribe through the OB&V process. ***Onboarding*** included the activities required prior to deployment. These include activities such as:

- Completing CSAT and NCIC Training and Certification
- Applying for and receiving LEEP Accounts
- Assigning Terminal Agency Coordinators (TAC) for each participating Agency
- Signing User Agency Agreements, TAP Addendum, Information Exchange Agreements
- Select Workstation Configuration
- Conducting Site Survey
- Actively Supporting and Participating in Technical Preparation

Vetting on the other hand was the process of applying for and receiving legal authority from FBI CJIS for an agency to access Criminal Justice Information (CJI) for a specified purpose. That authority comes via the assignment of a unique identifier for each agency, called an Originating Agency Code (ORI), that allows the agency to access various national crime information databases. The process is largely one of submitting various types of documentation to FBI CJIS and signing agreements such as an MOU for payment of civil fingerprint-based transactions. In addition, each agency had to have in place a comprehensive background investigation policy to demonstrate that the appropriate background checks are conducted on personnel prior to granting access to CJI. As an example, CJIS policy requires the documentation outlined below in order to issue an ORI to a law enforcement criminal justice agency. This documentation enables CJIS to make a determination as to whether access should be granted pursuant to federal law.A sample checklist of documents required by a Law Enforcement Criminal Justice Agency is below.

Requirements for: Law Enforcement Criminal Justice Agency

- ☐ **Proof that the primary function of agency is the administration of criminal justice** - Agency must provide documentation that shows the agency’**s** primary function is the administration of criminal justice; more than 50% of the agency’s functions must be devoted to the administration of criminal justice, as opposed to civil or administrative functions. This information must include what the criminal justice duties, functions, and powers of the agency or the subunit are, as well as the underlying authority granting these powers.

- ☐ **Proof that the primary budget allocation of the agency is for the administration of criminal justice** – Agency must provide documentation demonstrating it allocates more than 50% of its annual budget to the administration of criminal justice.

- ☐ **Proof that the agency has arrest powers** – Agency must provide documentation shows it has arrest powers pursuant to an executive order, statute, code, ordinance, or other underlying authority.

- ☐ **Proof that agency is a Law Enforcement Criminal Justice Agency whose officers have completed the required training** – Agency must provide documentation that describes their agency’s law enforcement training requirements established by the underlying authority that grants the arrest powers.

- ☐ **Proof that the agency has policies and procedures in place that comply with the “Minimum Screening Requirements for Individuals Requiring Access to CJI” as set forth in the CJIS Security Policy and that comply with name-based records check of personnel with CJI-access on a frequency of no more than every five years.**

Tribes had to complete all required OB&V milestones before they were considered ready for deployment.

3.3 Whole of Government Decisions

Initially, the TAP team attempted to conduct the OB&V process at the tribal level. However, once the process began, it became apparent that much of onboarding and all of the vetting process would actually take place at the agency level instead. Once TAP began dealing with individual agencies, the issue of how agencies would work together to make the most effective use of the TAP resources arose.

3.3.1 Federal legal authorities

As new types of tribal agencies sought to be involved with TAP, the TAP team worked closely with FBI CJIS to determine what national crime information databases an agency would be allowed to access based upon federal legal authorities and authorized purposes. As an example:

A Government Social Service (GSS) Agency receiving funds under the *Indian Self-Determination and Education Assistance Act (25 U.S.C. 450)*, or the *Tribally Controlled Schools Act of 1988 (25 U.S.C. 2501)* that conduct background checks of potential employees or volunteers that have contact or control over Indian children may:

- Conduct fingerprint-based criminal history background checks to national criminal database and receive an Identity History Summary (the criminal history rap sheet) or a "No Record Exists" report in response
    - Fingerprint-based criminal background check may be performed on:
        - Employees, prospective employees, or volunteers in positions that involve regular contact with, or control over, Indian children
        - Employees, prospective employees, or contractors in positions that do not involve regular contact with, or control over, Indian children but who require access to Criminal Justice Information as part of their employment

Under the Federal legal authority *Indian Child Protection and Family Violence Prevention Act Public Law 101-630 25 U.S. Code §3207*

The TAP team worked closely with FBI CJIS Office of General Council (OGC) to identify the legal authorities and authorized purposes for civil usage.

3.3.2 Data Decisions

Tribes were also charged with deciding what information they wanted to contribute to national crime information databases. Tribal governments were required to make legislative or policy determinations to provide guidance to tribal courts and tribal law enforcement about data sharing. Entering information into national crime databases may:

- Prevent prohibited persons from purchasing firearms;
- Enable officers across the country to have knowledge of tribal orders of protection, register sexual offenders, find missing juveniles, or to recover stolen property; and
- Indicate the status of a person (such as wanted, missing, endangered, sex offender, gang member) or property (stolen, lost, or recovered)

Entry of some information into federal criminal information databases requires certain responsibilities of the submitting agency. For example, entering person or property data into NCIC requires that the agency submitting the data be available 24/7 for "hit confirmation" in the event the person or property is located by another agency. A "hit confirmation" is used to:

- Confirm the person or property is identical to the person or property specified in the record;
- Confirm the warrant, missing person report, protection order, or theft report is still valid and outstanding; and
- Authorize an arrest, detention, or extradition of a wanted person; decide how to handle a missing person; decide to seize stolen property, or to process information concerning the return

of stolen property to the rightful owner; and decide how to process information concerning the terms, conditions, and service of an order of protection

Tribes had several options to meet the 24/7 hit confirmation requirement including: a) staffing a 24/7 dispatch center which monitors system messages, b) having an on-duty staff or on-call staff immediately available on a duty cell phone, or c) entering into an agreement with another law enforcement agency outside their jurisdiction to provide 24/7 access on the tribe's behalf.

Another decision to be made regarding data inclusion was consideration of legacy/historical records of arrests, orders of protection, and dispositions that had not been previously submitted to the FBI. The TAP workstation is equipped with a flatbed scanner capable of processing inked cards so that a tribe could enter retroactive information as well.

Many tribes, especially those without detention facilities, collaborate with local or county officials to detain subjects arrested by tribal police. This brought up the accompanying discussions regarding which jurisdiction would perform the arrest booking and submission of fingerprints, palm prints, and scars, marks, and tattoos and which ORI would be used for submission. These are important decisions, as the final court disposition for those arrests must be entered using the ORI under which the arrest was entered.

3.3.3 Service Models

Tribes were required to make decisions regarding who would enter information (e.g. each agency enter their own data or one agency enter on behalf of others) and which individuals would have access to Criminal Justice Information (CJI). Because CJI is controlled, there are policies regarding its transmission, storage and destruction as well as constraints on who can view CJI. These decisions would then impact decisions regarding placement of the workstation itself, so that it is in the most convenient, secure and safe location for the users.

The *Service Model* defines which agency will perform name-based and fingerprint-based checks and how CJI will be exchanged. There are three basic service models:

1. ***Self Service -*** Each agency performs fingerprint-based or name-base checks for themselves. All agency users must be authorized to access CJI, which requires that they complete CSAT training and have themselves completed a fingerprint-based background check.

2. ***Servicing Agency provides Criminal Justice Information to a Serviced Agency -*** A serviced agency with a TAP issued ORI utilizes another DOJ TAP based ORI agency (servicing agency) to perform all legally authorized transactions utilizing the TAP workstation on their behalf.

   A variant of this model is the use of "detailees." A serviced agency utilizes detailees from another governmental agency (servicing agency) as long as the serviced agency has management control over the detailee through an *agency-to-agency detailee agreement*.

3. ***Servicing Agency Provides "Go/No Go" Decision to Serviced Agency -*** This model allows the serviced and servicing agencies to adopt a "Go/No Go" model for name-based and fingerprint-based record checks. The serviced agency decides the criteria that would disqualify a candidate if found in their criminal history and provide that list of disqualifiers to the servicing agency. The servicing agency would then conduct the name-based or fingerprint-based background check on behalf of the serviced agency and provide them only a "Go" or "No Go" answer based upon the list of disqualifiers.

   In this model, no CJI is exchanged. The servicing agency may not disseminate any details of the criminal history record to the serviced agency, only a "Go" or "No Go." However, other than the Terminal Agency Coordinator (TAC) of the serviced agency, employees of the serviced agency do not need to meet background, training, or testing requirements for CJIN systems, because they do not have access to CJI.

If either model two or three is selected, the agencies must establish information exchange agreements (IEA) based upon the servicing model selected. These IEA must explain how CJI will be transferred, stored, and destroyed. In addition, internal audit processes that the serviced agency has to perform to ensure compliance with TAP regulations by the servicing agency must be outlined.

3.4 Deployment Process

A tribe's scheduled deployment date was selected 6-8 weeks in advance to allow for ordering and configuration of the workstation, as well as to ensure that network connectivity was in place and tested.

Deployment of the TAP workstation and training were accomplished in most cases in a single day. One tribe's deployment took a second day to complete due to the number of users to be trained. In the morning, the TAP trainers trained all agency participants together; the agenda included information about national crime information databases and their interrelationships, legal authorities for access, how to read a criminal history, handling of CJI, and scenario-based exercises that included all agencies, criminal and civil together. In some cases, this training session was the first time members of the various agencies had ever come together regarding their usage of TAP. During this introductory session, assumptions or previous whole of government decision were often challenged due to new voices expressing valid points of view and new service models or workstation location were proposed.

During the introductory training, the hardware vendor set up, configured, and tested the workstation in the designated area. In the afternoon, students were divided into groups for hands-on instruction on use of MESA, the biometric peripherals, and how to send a transaction to NGI. The other group was given more in-depth training in OpenFox Messenger (for person or property information) and how to access NCIC, III (for name-base criminal histories), or Nlets (for interstate records e.g. driver's license or registration information). Afterwards, the groups switched to ensure full training by all potential users.

OTJ, SMART, FBI CJIS, and other stakeholders joined and actively participated in deployment day training for the tribes, bringing expertise and counsel in areas related to their specialties. Deployment day ended with all agencies coming back together for a "whole of government" session to discuss issues, questions, or concerns that arouse during the day. It was found to be more productive if the agency leadership was present during these discussions.

3.5 Post Implementation Support

One of the lessons learned from earlier DOJ pilots was that tribes have varying sizes of IT staff that can be dedicated to the support of a program. In addition, without follow-on support, some pilot tribes stopped using the resources after a period of time due to staff turnover and loss of knowledge. Therefore, the TAP program instituted several initiatives to provide support following deployment day.

1. Maintenance and support for the workstation is provided by DOJ through the vendor's Customer Care Center (CSC). The CSC staff are available 24/7 for any issues related to the workstation, hardware peripherals, or any of the workstation software.
2. To address the issue of staff turnover or loss of knowledge, TAP designed the online CJIN Training and Learning Center, which contains training material, videos, facts sheets, and job aids to support on-the-job training, certification of new staff, or refresher training for those may require it.
3. The TAP team held biweekly teleconferences for all User Feedback Tribes and their agencies. TAP team members, as well as representatives from OTJ, SMART, and FBI CJIS were regular participants in these meeting. The meetings discussed challenges and issues, shared best practices, and recommended solutions, as well as provided education on a number of issues.
4. The Business Relationship Managers (BRM) played a large role in post-implementation support for their assigned tribes. BRMs assisted tribes in resolving internal process issues, helped to obtain ORIs for agencies that had issues, and addressed other organizational level challenges.

This level of post-implementation support is a key factor in the future success of the program, because it provides tribes with continued support, training and assistance that ensures continued use of the program.

3.6 Challenges/Lessons Learned during the User Feedback Phase.

Both TAP and the tribes experienced challenges during the OB&V process. The TAP team did not have an OB&V infrastructure or well-defined procedures and documents in place when TAP began. Thus, the TAP team developed "Vetting Packages" which contained documentation; Reimbursable Agreement templates; and checklists to include required documentation lists for criminal justice agencies (CJA), non-law enforcement CJAs, and non-CJAs needed to receive access authority from FBI CJIS. The TAP team also developed "Onboarding Packages" to ensure all pre-deployment activities were completed. These consisted of documentation that included a CJIN Workstation Configuration form; IT Review Checklist; Checklist for a Physically Secure location; Technical Specifications for OFM on a PC; User Account Spreadsheet; Templates for Background Investigation Policy, User Agency Agreement and TAP Addendum; and templates for Interagency Agreements. In addition, the TAP team developed, recorded and posted the online training modules, job aid, fact sheets, and CJIS Security Awareness Training and

Certification and the NCIC Training and Certification required for access to Criminal Justice information and access to NCIC.

One of the most immediate challenges during the OB&V period was the length of time it took tribes to complete the OB&V requirements. Initially the TAP team approached the OB&V process at the tribal level and planned to process nine tribes, estimating that no more than 30 days would be required for each. However, in reality, each tribal agency had to undergo separate vetting and partially separate onboarding. This increased the real workload from nine tribes to sixty-five agencies. In addition, some agencies took much longer to complete the OB&V process. Reasons for this varied but included:

- Difficulty collecting the required documentation for submission when applying for an ORI
- Difficulty collecting the signed documents such as UAAs, TAP Addendums, and IEAs
- The fact that each agency was undergoing OB&V separately meant that the tribe as a whole generally could not move forward until the majority of agencies received ORIs (we did in some cases move forward, while still waiting for ORIs for some agencies)
- Civil agencies took longer to vet because Reimbursable Agreements (RA) for payment of civil fingerprint-based background check fees had to be put in place between the tribes and CJIS. This process took anywhere from four to sixteen weeks
- Meeting requirements for physical security (e.g. secure, locked area) for the TAP workstation; several tribes had to specially install and configure internet connections and/or prepare secure areas for the TAP workstation
- Technical issues related to the tribe's IT staff providing the public facing Internet Protocol (IP) address led to delays in personnel from the tribe being able to access the online training/certification. There were further issuing in identifying and collecting the required information to create training/user accounts for all the users resulting in delays with personnel actually completing the training in a timely manner. All individuals attending deployment day training were required to, at a minimum, complete the CJIS Security Awareness Training
- Working through some of the 'whole of government' decisions which required careful consideration of which agencies would be participating, how they would share information, and the location of the workstation
- Having a tribal POC that was not at the executive level and thus could not enforce actions or milestones from agency heads, when needed

One final limitation was that the participating tribes would be accessing national crime information databases as federal users, and thus were subject only to uses authorized by federal law, not state law. The TAP team worked closely with FBI CJIS Office of General Council to identify appropriate federal authorities under which tribal civil agencies such as Child Social Services, Tribal Public Housing, and Child Protective Services could access national crime information databases for the purpose of conducting background checks.

Process improvements from these challenges and lessons learned are being incorporated into the FY17 Phase of TAP. The TAP team has a robust OB&V process with templates, better understanding of the technical challenges onsite, several well understood service models for interagency cooperation, a good understanding of current federal legal authorities and their boundaries, and nine deployed tribes who are available for advice and support to make FY17 a very good year for TAP.

4 Metrics and Success Stories

From February through the end of August 2016, the TAP team completed deployment to nine tribes with sixty-two separate agencies. Each agency required a separate package of information be collected, analyzed and approved for submission to CJIS. TAP collected monthly usage statistic of OpenFox Messenger (NCIC, III, and Nlets) as well as NGI (fingerprint-based submissions). These data collections were followed up with tribal discussions on usage trends, both high and low. As of October 2016, usage for major categories included:

- Register Sex Offenders: +110 Sex Offender related transactions
- Enter Orders of Protection: +350 Orders of Protection related transactions
- Prevent Inappropriate Gun Transfers: +115 disqualifying entries to prevent prohibited persons from purchasing firearms
- Conduct Fingerprint Checks: +300 fingerprint submissions both civil and criminal purposes
- Perform Investigative Use: +1,000 NCIC transactions/month

The usage varies from tribe to tribe and from agency to agency within each tribe. In some cases, tribes and agencies are still working through policy issues/challenges and have not been able to use TAP for specific agencies yet. In other cases, low usage is an indicator that, for the agency in question, state access is still serving their needs. For example, some tribes are continuing to use state access to NCIC for law enforcement/dispatch but use TAP for civil access to NCIC. In other cases, tribes that use county or local jails for detention following tribal arrests are still working out logistics of the arrest booking and ORI usage. TAP will continue monitoring usage and BRMs will follow up with tribes on a quarterly basis to discuss usage and understand if there are obstacles or challenges the tribes are facing, or if the reported usage is within normal range.

4.1 Success Stories

Regular tribal entry into and retrieval of data from national crime information databases should be considered a success on its own. However, the following are just a few of the success stories from tribes utilizing TAP given the lengthy history of tribal inability to access databases.

4.1.1 National Instant Criminal Background Check System (NICS)

NICS is the system used by gun dealers, also known as federal firearms licensees (FFL), to prevent prohibited persons from purchasing firearms. NICS checks a number of national criminal information systems such as NCIC and III to identify disqualifying factors such a felony convictions or other items as part of the normal administration of criminal justice. It also searches the NICS Index, a special database where disqualifying information may be entered for a number of other prohibitive categories such as professionally adjudicated mental health issues or drug abuse (court adjudicated or self-admitted). Items in the NICS index are prohibitors not normally captured as part of the regular administration of criminal justice

NICS Entry – Mental Health

A Tribal police department successfully entered a subject into the NICS Index under the prohibitive category of Mental Health following his acquittal at trial by reason of insanity. As a result, if this individual attempts to purchase a firearm, the FFL will now receive a "Denial – Do not proceed" answer and the individual will not be able to purchase a firearm. This capability was not available to the tribe through the state system.

NICS Entry: Domestic Violence

The TAP team and the NICS Program Office assisted a tribal police department with entering a subject into the NICS Index under the prohibitive category of Misdemeanor Crime of Domestic Violence. The tribal police believed there was an urgent need to enter the subject's disqualifying conviction directly into the NICS Index as soon as possible because they felt the subject posed an imminent threat to his spouse/former spouse. They knew the subject wanted his guns back after the case was adjudicated and was likely to try to purchase a weapon when they were not given back to him. There were also previous life-threatening actions taken by the subject against his spouse/former spouse. Now if the individual attempts to purchase a firearm, the gun dealer will receive a "Denial – Do not proceed" when the mandatory check is performed in NICS.

4.1.2 Orders of Protection

One tribe has entered all of their active civil Orders of Protection into NCIC via TAP. Previously, victims of domestic violence who received an Order of Protection from Tribal Court were required to hand carry the order to the local sheriff's office for entry of the order into NCIC on the tribes' behalf. Once TAP was in place and the tribal court was able to independently enter orders of protection, the Tribe's General Council noted, "this is excellent protection for the victims of domestic violence."

4.1.3 N-DEx: Recovery of Kidnapped Victim

A detective sergeant with a tribal police department was investigating the kidnapping of a vulnerable adult, but had only a potential name of the suspect. He logged on to the National Data Exchange (N-DEx) System and found a police report from another county that contained the full name and date of birth of the suspect. This new information indicated that another victim had an active protection order in place against the suspect. When that victim was contacted, he provided associated vehicle information that allowed the investigator to efficiently track down the suspect and locate the vulnerable adult. Without the N-DEx System, the investigation would have taken much longer and the possibility that the vulnerable adult would not have been located and recovered was very real.

5 Next Steps

DOJ is expanding TAP, making it available to additional tribes in FY 2017. Requirement for FY17 participation include:

- Tribe must be federally recognized
- Tribe must be a SORNA tribe with the responsibility of running an Adam Walsh Sex Offender registry or a tribal law enforcement agency that is not a BIA direct service agency
- Tribal government's express willingness to participate
- Tribe must have internet high speed access

As in the first phase of TAP, the application document is the "Expression of Interest" which is a letter or resolution from the tribe's governing body which includes:

- Name and contact information of a senior tribal executive who will act as the primary TAP point of contact. This individual must have authority to ensure coordination of TAP across various tribal agencies, departments, and offices. An alternate POC must also be named.
- A statement acknowledging that misuse or non-use may result in TAP access being discontinued.
- Language affirming the tribe's agreement to:
    - Make whole-of-government legislative and policy determinations, which provide guidance to tribal agencies about how national crime information databases are used, including what tribal data is entered into those systems.
    - Use TAP to close gaps related to access to national crime information databases if that was an impediment to the implementation of SORNA. This must be accomplished within one year of deployment.
    - Execute a memorandum of agreement with FBI CJIS and pay the standard national user fees associated with fingerprint-based for noncriminal justice (civil) purposes.
    - Provide necessary documentation and establish appropriate policies during the OB&V time period.
    - Ensure users of TAP establish appropriate accounts, take required training, background checks, and obtain necessary certification during the Onboarding and Vetting time period.
    - Ensure users of TAP participate in deployment day training during the deployment time period.
    - Comply with and adhere to auditing and policy requirements as well as all personnel, physical, and technical security requirements.
    - Provide high-speed Internet access to the workstation.

Key dates include:

- October 24-December 2, 2016: Expression of Interest submission period
- December 16, 2016: Notification to selected tribes

- December 19-May 31, 2017: Education and onboarding and vetting
- May 9-September 29, 2017: Deployment to selected tribes