



Job Aid | TAP Workstation Placement and IT Requirements

Purpose: To provide the Tribal POC and IT POC with information on Tribal Access Program (TAP) software, hardware, and documentation that should be submitted to the TAP team for successful set up. Your TAP Business Relationship Manager (BRM), will be hosting a series of meetings to walk you through this entire process which consists of the steps listed in the Table of Contents below.

TAP offers two solutions: TAP-LIGHT and TAP FULL. TAP-LIGHT provides agencies with the ability to conduct name-based record checks via the Justice Web Interface to NCIC (JWIN). Sections I and II and Appendix A of this document specifically apply to TAP-LIGHT Tribes.

TAP-FULL provides the Tribe with access to JWIN and the TAP Workstation to conduct fingerprint-based criminal & non-criminal justice record checks and submit arrest booking data.

I.	Access the JCIS Training and Learning Center.....	2
II.	Tribally Owned PCs - Access to NCIC.....	3
III.	TAP Workstation Location Selection	4
IV.	TAP Workstation Specifications	5
V.	TAP Workstation Environmental Specifications	6
VI.	TAP Workstation Connectivity Specifications	7
VII.	Site Survey and Connectivity Test Meetings	7
VIII.	Training Room Requirements: Week of On-Site Training.....	9
IX.	Order Fingerprint/Palmprint cards from FBI CJIS	10
X.	Workstation Delivery	11
XI.	Workstation Installation Day	12
XII.	TAP Workstation Training Agenda	13
XIII.	Post –Deployment IT Support	15
XIV.	TAP Workstation Moves	16
XV.	Onboarding and Vetting Checklist for the TAP Workstation	17
	Appendix A: IT Related JCIS Documentation.....	18

Job Aid | TAP Workstation Placement and IT Requirements

I. Access the JCIS Training and Learning Center

The public IP address of any system that will be accessing csa.justice.gov is requested so DOJ may authorize access through the DOJ firewall.

Please provide the following by emailing to TribalAccess@usdoj.gov:

1. The public IP address of the network location that will host the TAP Workstation and Printer.
2. The public IP address of any Tribal system that will be accessing csa.justice.gov
3. If you have Dynamic IP addresses as your Public IP, we need the range of all possible IP addresses that would be the public IP for #1 and #2.

Note: DOJ cannot provide access to private or personal IP addresses. Please do not send a private or personal IP address.

Private IP address ranges include:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Once you receive notification that your IP addresses have been added to the firewall, please confirm that the Tribe can access the Justice Web Interface to NCIC at csa.justice.gov (see Figure 1). A successful connection will verify inclusion of your Public IP to the DOJ firewall whitelist.

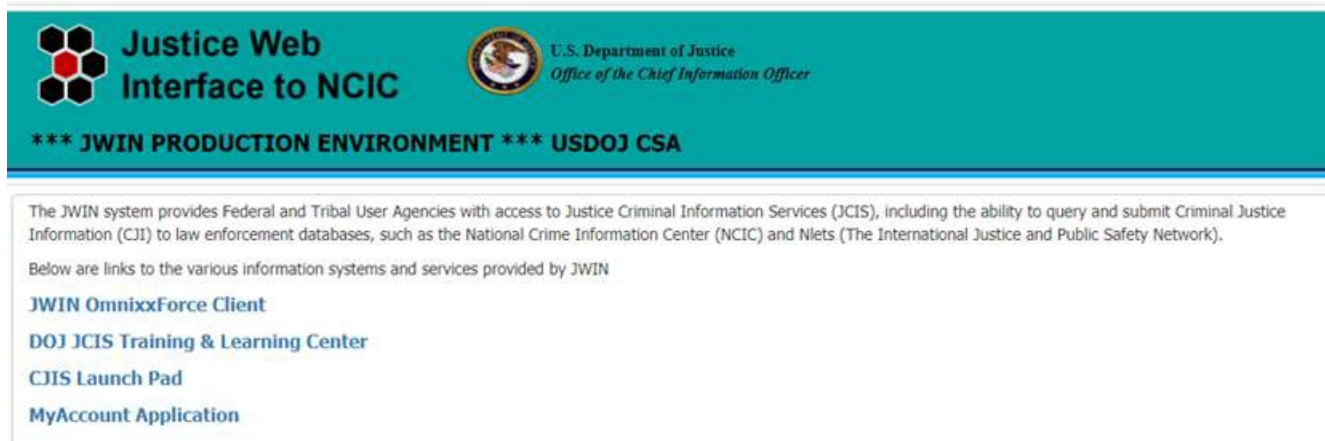


Figure 1: Justice Web interface to NCIC

II. Tribally Owned PCs - Access to NCIC

It is the Tribe's responsibility to ensure that any network that has access to criminal justice information is the Tribe's responsibility to ensure connectivity and is in compliance with FBI CJIS Security Policy. The most recent version of the CJIS Security Policy can be found online at www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

All devices, networks, and persons that will have access to Criminal Justice Information, which includes storage, transmission, and physical location, shall also be in compliance with the most recent version of the CJIS Security Policy v5.9.

Familiarization with the CJIS Security Policy is required as it provides a baseline of security policies and procedures, and much of what is in there is a broad description of how to operate securely. Below, we have highlighted important areas to consider.

1. Session Lock/ Screen Lock: The information system shall prevent further access to the system by initiating a session lock after a maximum of 15 minutes of inactivity¹, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
2. Authentication: There are numerous CJIS Security Policy acceptable methods of authentication, the most common is a username and password, with a minimum password length of 12 characters, which must include a number, symbol, lowercase, and uppercase characters.
3. Malicious Code Protection (Virus Protection): The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).
4. Boundary Protection (Firewalls and Network Segmentation):
 - a. Control access to networks processing CJI.
 - b. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
 - c. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).
 - d. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
 - e. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the setting should be set to "fails closed" vs. "fails open"). This would prevent unauthorized traffic if the boundary protection fails.
 - f. Separate publicly accessible information system components (e.g. public Web servers) from your criminal justice networks.

¹ FBI CJIS Policy requires session lock after 30 minutes while [DOJ's Standard for Unclassified Systems](#) requires session lock after 15 minutes of inactivity. See AC-11 and AC 11-01(01) for relevant requirements.

III. TAP Workstation Location Selection

Decisions on where to place the TAP workstation should be made by Tribal Leadership and the TAP POC. The workstation location needs to be accessible by the SORNA Officer and all other TAP participating agency personnel as each agency authorizes. The IT POC's role is to ensure the Workstation location will be able to be adequately supported by your network. The POC, TAC, and IT POC will ensure the location meets the requirements outlined below. **Send photos or a video of the location that has been selected and the route through the building that delivery must take. This is so that the TAP team can verify if the location meets the physically secure location requirements, and so that the shipper can better prepare delivery requirements (e.g. Stairs, narrow hallways). Note: The workstation should not be moved after initial delivery without prior coordination with DOJ/TAP since this may void the warranty with the vendor.**

Physically Secure Location Checklist for the TAP Workstation

Agencies must ensure the following provisions are met in order to meet the requirements of a physically secure location as defined by the CJIS Security Policy v5.9, Section 5.9:

"A physically secure location is a facility, a police vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect Criminal Justice Information (CJI) and associated information systems. The physically secure location is subject to criminal justice agency management control; State Identification Bureau (SIB) control; FBI CJIS Security Addendum; or a combination thereof."

- ☐ Prominently post signs designating the building/office as a physically secure area
- ☐ Maintain a list of personnel with authorized access/issue credentials to authorized personnel
- ☐ Maintain control of all physical access points and verify individual access authorization before granting access
- ☐ Maintain physical control over all areas where equipment is located (computer, wire closet, etc.)
- ☐ Ensure computers are positioned in such a way that unauthorized individuals cannot view it
- ☐ Ensure all those with access to the physically secure area have completed the appropriate security awareness training
- ☐ Monitor physical access and respond to physical security incidents
- ☐ Authenticate visitors before they enter the physically secure area / Escort visitors at all times and monitor visitor activity
- ☐ Authorize and control the movement of physical equipment in/out of the physically secure area

If an agency is unable to meet all of the requirements listed above, they may place the CJI equipment and printed material in a separate internal office/area with limited access that meets the following requirements as defined by the CJIS Security Policy v.5.9, Section 5.9.2, Controlled Area:

- ☐ Limit access to agency personnel that are authorized to access/view CJI
- ☐ Ensure all those with access to the physically secure area have completed the appropriate security awareness training
- ☐ Lock the office/area when unattended
- ☐ Position the equipment and printed material containing CJI in such a way that prevents unauthorized viewing
- ☐ Follow the encryption requirements found in the CJIS Security Policy, Section 5.10.1.2 for electronic storage of

IV. TAP Workstation Specifications

TAP Full will provide a Workstation, Printer, and Scanner these items will require a secure location, power, and a reliable and secure connection to the internet. The updating and servicing of those two devices is the responsibility of TAP.

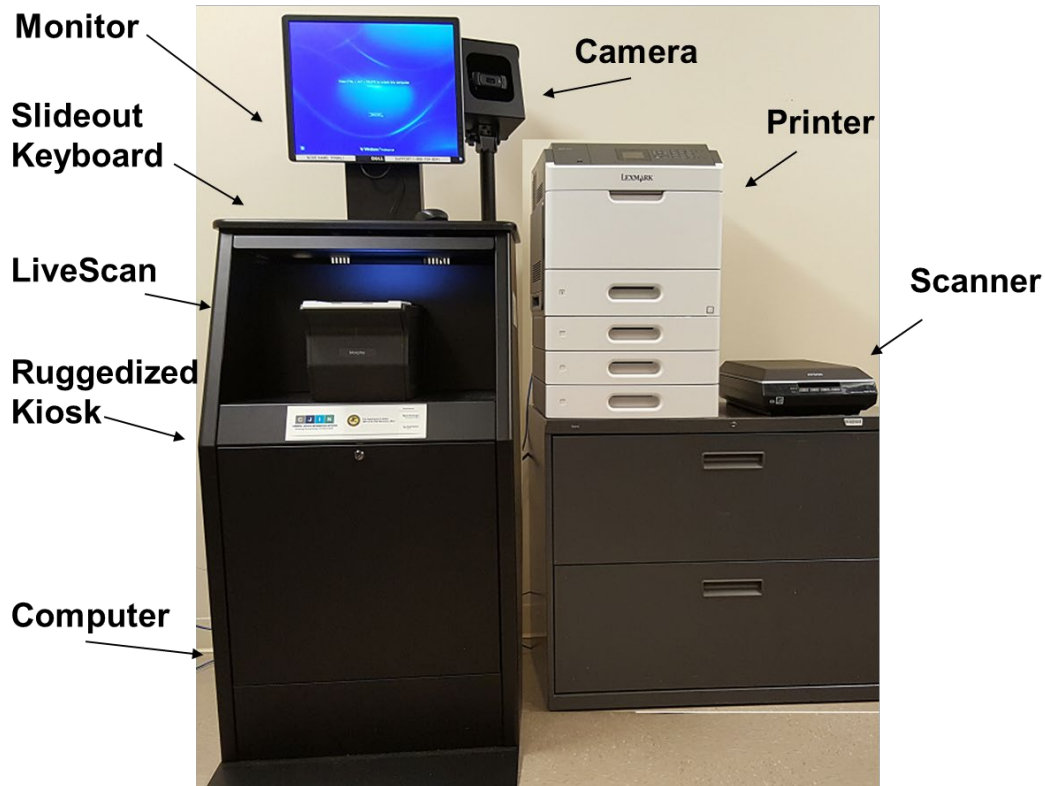


Figure 2: TAP Workstation Equipment

The workstation is shipped with the following:

- DOJ PC: Dell OptiPlex 7060 Micro
- Monitor: Dell P2219H
- Live scan device: IDEMIA TP5300A-ED 500PPI
- Webcam camera: Logitech C920
- Flatbed scanner: EPSON V800
- Printer: Lexmark MS823DN
- Universal Power Supply
- Miscellaneous: Keyboard, Mouse, Cables

V. TAP Workstation Environmental Specifications

The room where the workstation will be placed needs to also have the following in addition to meeting the CJIS Physically Secure Location requirements:

- Desk or Table to hold:
 - Flatbed scanner: EPSON V800
 - Dimensions: 12.1" x 19.8" x 6" (W x D x H)
 - Weight: 14.6 lbs.
 - Printer: Lexmark MS823DN
 - Dimensions: 16.75" x 20" x 27" (W x D x H)
 - Weight: 85.2 lbs. (excluding paper)
- Environment
 - Ambient temperature range (operating): 59 – 92°F
 - Relative humidity range: 20-85% (non-condensing)
 - A/C should be away from workstation
- Telephone (Recommended)
 - Ensure telephone service is available from the room where the workstation will be placed. This can be a cellular network if there is adequate service; land line or Voice Over IP (VoIP) is recommended otherwise to ensure users have the ability to communicate with Tier 1 Help Desk services for TAP
- Power
 - Dedicated 20 amp, 110volts +/- 10 volts, 60 Hz grounded receptacle at workstation location
- Lighting for taking photos for bookings and sex offender registration
 - Workstation should not be directly beneath the overhead lighting, but area should be well-lit for pictures
 - Three-point lighting is ideal to avoid shadows falling across the face
 - At least 6 feet of clear space around the workstation so that a subject can stand at least 3 feet away from the camera
 - Recommend that the subject stand in front of an 18% gray background for photos

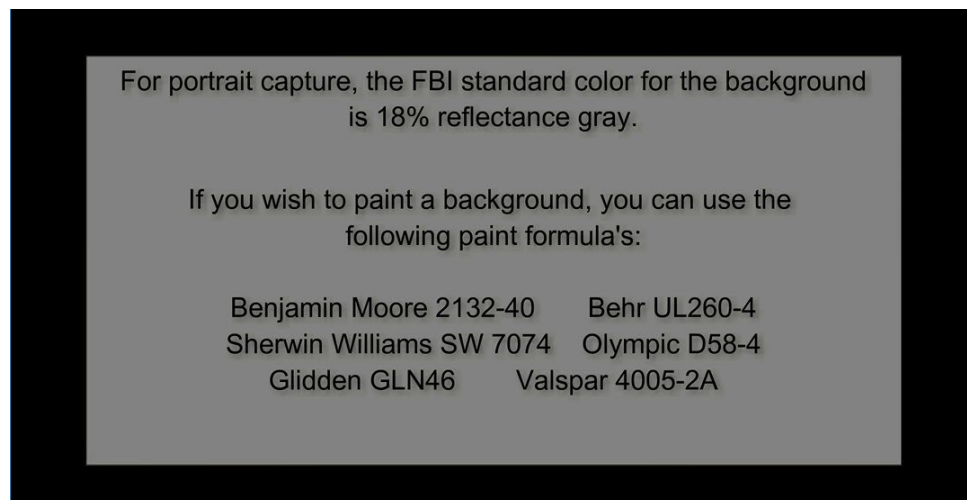


Figure 3 - Suggested paint colors for photos

VI. TAP Workstation Connectivity Specifications

The TAP Workstation PC requires wireline internet access. The TAP workstation does not support a wireless connection. The TAP Workstation printer requires a separate IP address for connection to the PC. The IP address for the printer must be on the same network as the IP address that is used for the TAP Workstation PC with the MESA software.

TAP Workstation Network Requirements

1. The Tribe may host the TAP Workstation on the existing Tribal IT network, or the Tribe may provide a dedicated ISP connection for the TAP Workstation
 - a. May include additional costs for the Tribe
 - b. Bandwidth dedicated to the TAP Workstation
 - i. Recommended: 3 MBps
2. Two RJ45 Network connections to the Tribes local network
 - a. One RJ45 connection for the TAP Workstation location
 - b. One RJ45 connection for the TAP Printer location
 - c. The Workstation and Printer are standalone devices on your network; they shall not be file sharing within your network and are only utilizing the internet access.
3. 1 Static Private IP Address: Used for the TAP Workstation
 - a. Requires access to the Internet
4. 1 Static Private IP Address: Used for the Printer
 - a. Requires access to the Workstation.
5. Two RJ45 Network Cables needed
 - a. Printer: Connect the printer to the Local Area Network (LAN)
 - b. Workstation: Connect the PC in the workstation to the LAN
 - i. The cable lengths will depend on the location of the devices (printer or PC) and the location of the LAN drop for each.
6. Ports 80, 443, 1935, and 5832 need to be open for outbound and inbound TCP traffic on your boundary protection; all other traffic shall be controlled and limited based upon your operational requirements.

VII. Site Survey and Connectivity Test Meetings

A site survey meeting will be set approximately 6 –8 weeks before the arrival of the TAP workstation to review IT related requirements with the TAP POC and IT POC. This includes reviewing an overview map of the building (e.g. are there stairways), photos of the room and hallways where the workstation will be located. The location of the workstation must again meet the physically secure checklist as well as meet the internet access and environmental specifications above.

The Site Survey meeting requires the Tribal and IT POC to be present and will cover:

- Review of location selected for the workstation and workstation order form
- Review physical security checklist and recommendations for ensuring security
- Status of internet connection and process for scheduling a connectivity test
- Process for ordering blank fingerprint cards
- Questions regarding workstation installation and delivery

A connectivity test will be set up approximately 4-6 weeks before the arrival of the TAP workstation and be conducted at the same time as the site survey. DOJ cannot ship the workstation until a successful connectivity test has been completed.

Job Aid | TAP Workstation Placement and IT Requirements

A Tribally-owned laptop computer and ethernet cable will be needed for connectivity testing. Tribal IT staff will need to bring the laptop to the physical location and network port identified for the workstation to complete the connectivity test tasks described below:

- Test connectivity with Justice Web Interface to NCIC csa.justice.gov
- Test internet access with the wireline IP address that will be used for the TAP workstation
- Test internet access with the IP address that will be used for your Devices that will access NCIC with JWIN, (Justice Web Interface to NCIC.)
- Test Workstation vendor's ability to remotely access the TAP workstation PC
- Test internet access at the training room that will be used during on-site training activities
- Confirm Ports 80, 443, 1935, and 5832 are not blocked. This is needed for JWIN, and LEEP to operate properly.
- Allow access to IP address: 12.217.12.72 to remote in and install the BeyondTrust client on the Workstation.
- Confirm ports 80, 443, 1935, and 5832 are opened for outbound and inbound traffic through your firewalls.
- Confirm phone service is available in the room where the TAP workstation is being placed
- Confirm that two RJ45 cables are available for use for the TAP workstation and printer
- Confirm a table is available for the printer and scanner
- Confirm fingerprint and/or palm print cards were ordered / received

VIII. Training Room Requirements: Week of On-Site Training

TAP requests the POC, TAC, and IT POC to assist in preparing for training. The Tribe's BRM will host a call with the Tribe prior to training to confirm the following. A list is included below to assist with your preparations.

Ensure the Training Room has Necessary Internet Access

On the day that DOJ comes on site to install the Workstation, the DOJ Trainer's laptop will need internet access in order to access criminal justice information through JWIN and LEEP.

We need the public IP address of the training location prior to our arrival, so that we may clear it through the DOJ firewall to facilitate training.

Some items to consider:

- Can you provide guest connectivity to the Tribe's network for the DOJ Trainer's PC?
- Do you have a DMZ (demilitarized zone) or perimeter network that can be used for the DOJ Trainer's PC to access the internet?
- Do you require a static IP address for the DOJ Trainer's PC to access internet through guest connectivity?
As a backup, we'd like to ask if the Tribe's IT department can let the DOJ Trainer use a PC that belongs to the tribe and is already connected to your network and has public internet access.

Classroom set up

In addition to connectivity requirements above, TAP requests that the TAP POC assist with the following:

- Identify whether there are two locations available for training breakout sessions
- Identify whether training will be conducted in classroom or computer lab-style rooms
- Confirm whether screen projector with HDMI hookup is available in the training room

IX. Order Fingerprint/Palmprint cards from FBI CJIS

Six to eight weeks before on-site installation day, the TAP POC or IT POC should order blank fingerprint cards and palmprint cards from FBI CJIS. There is no charge for ordering cards.

To place an order, navigate to the following site: <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ordering-fingerprint-cards-and-training-aids>

- You will need a CJIS assigned TAP ORI to place the order (e.g. Use the Law Enforcement ORI)
- You will have the option of ordering cards that have your agency's ORI pre-printed on them or not. Please order the ones that **DO NOT** have an ORI pre-printed on them because each box contains several hundred cards.

Order one (2000 card) box of each of the following card types:

- FD-249 Criminal Cards – Criminal fingerprint cards
- FD-258 Applicant Cards – Civil fingerprint cards
- FD-884 Palm Print Cards

On the day of on-site installation, the instructor will show users how to properly load the blank cards into the several paper trays and print out fingerprints and palmprints. The printer trays should also be labeled.

Job Aid | TAP Workstation Placement and IT Requirements

X. Workstation Delivery

When the TAP workstation has shipped, your BRM will notify the TAP POC, IT POC, and receiving individual if not one of the former. The Tribal representative receiving delivery must sign packing slip and send an electronic copy to TAP BRM.

The TAP workstation will be delivered, strapped to a pallet, and weighs over 200 lbs. It is best that the whole package be delivered to the location where it will be used. In addition, please make sure that the package can be maneuvered into the room where the system will be housed. The pallet is about 2 ½ - 3 feet wide. A clear path from where the truck can deliver the equipment to the room will be necessary. The remaining equipment (e.g. printer and scanner) will be delivered on a second pallet, weighing over 150 lbs.

Upon arrival:

- Contact your TAP BRM and let them know the workstation arrived
- Take photographs of both pallets, the one with the Workstation and the one with the other equipment. Send the photographs to the TAP BRM and cc: TribalAccess@usdoj.gov.
- Please do NOT open the protective wrapping and do NOT open any boxes. The Workstation vendor installer will do this when he / she arrives on installation day.
- Inspect the Workstation and equipment boxes. Do they look intact? Are there any visible signs of potential damage? Does the Tip N Tell indicator indicate damage? (see picture below)
- If there are any signs of damage, please contact the BRM immediately. DO NOT open the wrapping or boxes, we will be asking you to take photos and send them to DOJ for insurance purposes.
- Again, the Tribal representative receiving delivery must sign packing slip and send an electronic copy to your TAP BRM.



Job Aid | TAP Workstation Placement and IT Requirements

XI. Workstation Installation Day

The vendor will be on site at an agreed upon time to complete the set-up of the TAP Workstation; frequently this is approximately 8:30 am. A sample agenda is shown below.

We request that the Tribe have on hand a box-cutter, phillips and flat head screwdrivers.

Please designate an IT person who can address any technical issues that may arise.

Time / Event	
8:15 am – 11:30 am	TAP Workstation Installation Location: TBD Participants: Workstation Engineer, IT POC, Agency POC
11:30 am –12:30 pm	TAP Quality Control Check (TAP Workstation Delivery Checklist & Test a Real Fingerprint Transaction) Join Adobe Web Link: TBD Dial-in Conference Call Information: TBD Participants: Workstation Engineer, TAP BRM
12:30 – 1:30pm	Lunch on your own
1:30 pm – 4:00 pm Remote	TAP Workstation – Training with Workstation Engineer (See checklist below) Location: Workstation Room User information: NAME: 1:30 – 2:30 NAME: 1:30 – 2:30 NAME: 2:45 – 3:45
1:30 pm – 4:00 pm In Person	TAP Workstation – Training with Workstation Engineer (See checklist below) Location: Workstation Room User information: Ensure all users are able to log on the Kiosk and MESA.

XII. TAP Workstation Training Agenda

☐ Overview of Workstation Hardware

- ☐ Cabinet – how to open cabinet, how to turn on computer if shut down. Remind them to just log off.
- ☐ Livescan – for taking fingerprint and palm prints
- ☐ Camera – for bookings and sex offender registration
- ☐ Scanner – for scanning and submitting inked cards
- ☐ Printer – for printing fingerprint cards

☐ Demonstrate Windows login and provide overview of desktop

- ☐ Have users review and use the Account Cheat Sheet to setup passwords
- ☐ Locate MESA icon, LEEP icon, DOJ Helpdesk information, and EFT Directory
- ☐ Move MESA icon, LEEP Icon, EFT Directory, to center of screen as these will be the icons they will be using

☐ Login to MESA and provide overview of TOTs screen

- ☐ Review Criminal ToTs
 - Arrest Bookings
 - Inquiry
 - Sex Offender Registration
- ☐ Review Civilian ToTs
 - FANC – Criminal Justice Agency Employment Only
 - FAUF – CJA Volunteers, Employees with contact or control over Indian Children, Public Housing.
- ☐ Review Cardscan v. Livescan
- ☐ Hand out ORI/Reason Fingerprint Chart

☐ Demonstrate Livescan entry

- ☐ Complete FAUF or FANC Transaction (depending on training audience)
 - Have users take turns rolling fingerprints from start to finish.
- ☐ Discuss ORI and Reason Fingerprinted
 - FANC Transaction – use Police ORI and RFP = CFR 28 sections 20-33 A 1
 - FAUC Transaction – use Social Services or HR ORI and RFP = P.L. 101-630
- ☐ Discuss fingerprint problems, exceptions, dry fingers, retaking fingerprints and overriding.
- ☐ Save EFT file and demonstrate how to locate via EFT directory.
- ☐ Have users sign into LEEP and locate @leo.gov email. Explain that the file will be sent to the FBI for comparison of existing criminal fingerprints.
 - Note:** Only send a FANC transaction on a Criminal Justice Employee. Demonstrate without sending if conducting another transaction.
- ☐ Demonstrate printing cards

Job Aid | TAP Workstation Placement and IT Requirements

- ☐ Booking (if Law Enforcement are present)
- ☐ Have users take turns rolling fingerprints from start to finish.
- ☐ Discuss fingerprint problems, exceptions, dry fingers, retaking fingerprints and overriding.
- ☐ Demonstrate how to capture photos and SMTs and where to locate in EFT directory.
 - Note: Do not save or submit transaction.

☐ Demonstrate Card Scan Entry

- ☐ Using previously printed livescan entry, walk through the process of submitting a FAUF or FANC cardscan entry.
- ☐ Discuss ORI and Reason Fingerprinted
 - FANC Transaction - use Police ORI and RFP = CFR 28 sections 20-33 A 1
 - FAUC Transaction – use Social Services or HR ORI and RFP= P.L. 101-630
- ☐ Demonstrate how to upload photos from EFT directory.
- ☐ Demonstrate how to save EFT.
- ☐ Discuss process for submitting EFT via LEEP. Do not submit.

☐ Demonstrate Case Manager (even to non-admin)

- Inform users that transaction may be recovered, edited, and removed by admins

XIII. Post –Deployment IT Support

After initial on-site installation of the TAP Workstation it will be necessary for the vendor to access the TAP workstation remotely to service the software and hardware, for reasons such as the following:

- Edit configuration files and settings (e.g., add a new ORI provided by CJIS, add new users, update permissions for users)
- Install a new software release
- Apply software maintenance releases
- Remotely access the workstation to troubleshoot hardware and software issues (Tier 1 Help Desk personnel)

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 AnaheimCSCenter@us.idemia.com; Cc: tribalaccess@usdoj.gov
- Please include your Tribe's Name in the subject line of the email

XIV. TAP Workstation Moves

All workstation moves must be coordinated with the TAP team and vendor prior to the move. This is required to avoid voiding the warranty with the vendor for maintenance and support.

The Tribal POC should notify their TAP Business Relationship Manager that the Tribe intends to move the workstation and the timeline for the move.

The Tribe will be required to complete and submit a workstation move form along with photos.

The TAP team and vendor will provide instructions for safely completing the move and ensuring connectivity after. In some cases, the vendor will come onsite to assist with the move.

Before Move

While the TAP Workstation equipment is still at its current room (i.e., the old location of the Police Department) and before moving any of this equipment, please take the following photos:

- One or more photos of the current TAP Workstation location
- One of more photos of future TAP Workstation location, to include photos of new building (if applicable), potential obstacles to the move (stairs, narrow doorway, etc.)
- Please save these photos. Each of the photos will have a file name and a date when the photo was taken. Give each photo a filename like “BeforeMove 120120 Photo1”, etc.
- Send photos to BRM and cc: TribalAccess@usdoj.gov

After Move

After the TAP Workstation equipment has been moved to its new location, please take the following photos:

- Photos of new TAP Workstation location
- Please save these photos. Each of the photos will have a file name and a date when the photo was taken. Give each photo a filename like “AfterMove 120120 Photo1”, etc.
- Send photos to BRM and cc: TribalAccess@usdoj.gov

XV. Onboarding and Vetting Checklist for the TAP Workstation

This checklist is a summary of this document.

- ☐ Tribe POC and IT POC attend “TAP Workstation/IT Requirements” webinar
- ☐ BRM and Tribe discuss placement of workstation and Tribe ensures they follow the Physically Secure Location Checklist
- ☐ Tribe installs an ISP connection if necessary
- ☐ BRM to indicate if on a ☐ independent ISP connection or on ☐ Tribal Network
- ☐ Workstation will be located at: [Tribe to insert agency name and address]

If this Tribe is a SORNA Tribe, the workstation must be accessible to the SORNA Officer. Agreement from the SORNA Officer is required. Also, if the Tribe is conducting bookings, it needs to be in a place that is accessible to the Tribal agency responsible for performing this task.

- ☐ Tribe submits workstation order form and pictures to BRM by [BRM to insert date at least 10-12 weeks prior to deployment]
- ☐ Tribe to indicate any special considerations (stairs, small doorways) [Tribe to enter in data]
- ☐ BRM concurs with location
- ☐ DOJ submits to Vendor for processing
- ☐ Tribe/IT POC conducts IT Site Survey meeting with BRM by [BRM to insert date] (at least 8 weeks prior to deployment)

Notes/Action Items:

- ☐ Tribe/IT POC conduct connectivity test with BRM and vendor by [BRM to insert date] (at least 4-6 weeks prior to deployment)
- ☐ DOJ submits all ORIs and usernames to Vendor by [BRM to insert date]
- ☐ Workstation ships to Tribe on [BRM to insert date] Tracking Number: [BRM to enter in #]
- ☐ Workstation should arrive on [BRM to insert date]
- ☐ Tribe takes photos of Tip and Tell and emails signed and dated packing slip to BRM

Notes/Action Items if there was any damage:

- ☐ Tribe signs off on delivery receipt and returns to DOJ/TAP Team

Job Aid | TAP Workstation Placement and IT Requirements

Appendix A: IT Related JCIS Documentation

The following JCIS documentation is required to be completed by the Tribe. Links to each of the documents are provided in the table below.

Document Title	Document Description	Who needs to sign?
TAP Onboarding and Vetting Password: tribal2019	All Documents and Training Materials provided by TAP	Everyone who needs information about onboarding, documentation, and training related to TAP
TAP Addendum for TAP-FULL	Outlines responsibilities regarding agency and LEEP, providing technical support and troubleshooting issues, Internet service, and moving the TAP workstation (DOJ will sign and return final copy)	One per Tribe, signed by agency head and agency TAC of the agency where the TAP workstation and/or JWIN is located
TAP Addendum for TAP LIGHT	Outlines responsibilities regarding agency, providing technical support and troubleshooting issues, Internet service, and moving the TAP workstation (DOJ will sign and return final copy)	One per Tribe, signed by agency head and agency TAC of the agency where the TAP workstation and/or JWIN is located
Local Agency Security Officer Addendum	Assigns a person to the position of LASO, who responsible for ensuring all information security requirements are met as it pertains to the protection of Criminal Justice Information (CJIS) accessed through the DOJ Justice Criminal Information Services (JCIS)	One per Tribe signed by IT POC
Information Technology (IT) Management Control Agreement	Establishes that the Criminal Justice Agency (CJA) has the responsibility to enforce priorities, physical, personnel and logical security requirements regarding the use and access to CJIS systems	One per Tribe, signed by each applicable TAC and IT POC
Sample IT Policy	Required that the Tribe has a policy and procedures in place to address system administration, network infrastructure and information protection.	One per Tribal IT agency and all ORI's they support
IT Quick Reference Sheet	A one-page list of network setting to host and access TAP hardware and systems.	IT Personnel who need details on network configuration in relation to TAP