



COMMISSIONERS COURT
COMMUNICATION

COURT ORDER NUMBER _____
PAGE 1 OF 19
DATE: 12/17/2024

SUBJECT: **CONSIDERATION OF A MEMORANDUM OF UNDERSTANDING/INTERLOCAL AGREEMENT BETWEEN TARRANT COUNTY CRIMINAL DISTRICT ATTORNEY AND STATE AGENCIES FOR THE PARTICIPATION OF INFORMATION SHARING VIA TECHSHARE.LEA AND TECHSHARE.PROSECUTOR**

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED

It is requested that the Commissioners Court consider a Memorandum of Understanding (MOU)/Interlocal Agreement (ILA) between Tarrant County Criminal District Attorney (CDA) and State Agencies for the participation of information sharing via TechShare.LEA and TechShare Prosecutor.

BACKGROUND

Since 2013, Tarrant County has been a participant in the TechShare Program. The Tarrant County CDA's Office uses the Techshare.Prosecutor system as its case management software in criminal cases. Law enforcement agencies utilize the Techshare.LEA portal to submit cases and evidence to the Criminal District Attorney's Office for prosecution.

This MOA/ILA memorializes the expectations and guidelines for the use of the data contained in TechShare between the CDA's Office and the University of Texas at Arlington Police Department ("UTAPD"). This agreement was requested by UTAPD as part of its certification process with the Texas Department of Public Safety.

With approval, the CDA's Office will continue to use the Techshare.Prosecutor system and continue to accept cases, data, and evidence submitted by UTAPD through Techshare.LEA.

The terms and conditions of this Agreement shall be indefinite unless terminated by one of the Parties.

The Criminal District Attorney's Office has approved this MOU/ILA as to form.

FISCAL IMPACT

There is no fiscal impact associated with this request.

SUBMITTED BY	Criminal District Attorney	PREPARED BY:	Polly Maxwell
		APPROVED BY:	Mark Kratovil

**MEMORANDUM OF UNDERSTANDING / INTERLOCAL AGREEMENT
WITH STATE AGENCIES AND TARRANT COUNTY CRIMINAL
DISTRICT ATTORNEY**

TO PARTICIPATE IN INFORMATION SHARING VIA
TECHSHARE.LEA AND TECHSHARE.PROSECUTOR

I.
PARTIES

This Memorandum of Understanding / Interlocal Agreement ("MOU/ILA") is entered by and between the undersigned State Agency of the State of Texas ("State Agency(s)"), acting by and through their respective Law Enforcement Agencies, pursuant to and under authority of the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code and for the purpose of sharing Criminal Justice Information ("CJI") via TechShare.LEA Portal ("LEA Portal") and TechShare.Prosecutor ("TSP") Applications. The undersigned State Agency / Law Enforcement Agency enters into this Interlocal Agreement ("Agreement") with Tarrant County Criminal District Attorney ("TCDA"). Any and all State Agencies of the State of Texas adopting this Agreement upon a formal order of their respective governing bodies as provided for herein may be referred to in this Agreement individually as "Party" and collectively as "Parties."

II.
RECITALS

WHEREAS, State Agency desire to enter into this Agreement to participate in the use of the LEA Portal to electronically file criminal cases with TCDA in TSP;

WHEREAS, State Agency will have access to the LEA Portal in order to file cases electronically, upload digital media evidence, search and share CJI, and perform other functions as allowed by statutes and role based permissions;

WHEREAS, TCDA agrees to provide access to the LEA Portal at no cost to State Agency and their designated Law Enforcement Agency personnel, and all Parties agree to abide by the terms and conditions laid out in this Agreement;

NOW THEREFORE, in consideration of the promises, inducements, covenants, agreements, conditions, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the State Agency and TCDA agree as follows:

III.

PARTICIPATION BY ADDITIONAL STATE AGENCIES

Any local government may participate in this Agreement with the signature of the designated authorized signer on the signatory page of this Agreement. Each State Agency will be required to approve and agree to the terms and conditions of this Agreement.

IV.

DATA OWNERSHIP, ACCESS, SECURITY AND STORAGE

- A. Ownership. TCDA owns the TechShare.Prosecutor and TechShare.LEA Portal software applications and has agreed to allow access to State Agency's LEA users. It is the intention of the Parties that each State Agency will remain the custodian and owner of its information and data that it created or submitted to TSP via the LEA Portal, unless expressly agreed in writing otherwise. The Parties acknowledge and agree that such information or data shall not be used by the Parties other than in connection with the performance of this Agreement or as contemplated by the Parties under this Agreement. Additionally, the Parties agree that the data shall not be disclosed, sold, assigned, leased or otherwise provided to third parties, or commercially exploited by or on behalf of the other Parties, their employees, officers, agents, subcontractors, invitees, or assigns in any respect without the expressed written approval of the State Agency that owns such data.
- B. Interfaces. Each Party is responsible for developing and maintaining its interfaces to the LEA Portal. State Agency is responsible for the cost of its own interface development and maintenance.
- C. Security and Access of Data.
- 1) Each Party is responsible for ensuring its employees and other persons accessing data within TSP via the LEA Portal are authorized to do so and will use such data only as is legally permitted, and as outlined in EXHIBIT A, attached herein.
 - 2) State Agency and their representatives agree that the following terms and conditions apply regarding access to the criminal justice information ("CJI") and data maintained in TSP:
 - a) State Agency and their representatives shall acknowledge and agree that the purpose of access to criminal justice information in the LEA Portal is to perform criminal justice related functions.

- b) State Agency agrees that the LEA Portal shall not be used for any personal purposes, including entertainment, personal business, or personal gain.
- c) State Agency understands that access to, and transmission of, any data or material deemed to be a violation of any federal, state, or local law or agency administrative rules is prohibited.

Survival. This Article IV shall survive any termination, cancellation, withdrawal, or expiration of this Agreement.

V. **TERMS AND TERMINATION**

The terms and conditions of this Agreement shall be indefinite unless terminated by one of the Parties. This Agreement may be terminated by either Party with a thirty (30) day written notice to the other Party.

VI. **WARRANTIES**

No Party to this Agreement warrants the availability, accuracy, quality, reliability or fitness for a particular purpose of any data or information made available under this Agreement. Third party warranties or guarantees may inure to the benefit of the Parties to a particular Project if such are contractually secured as apart of such Project; however, no Party to this Agreement shall be held liable for a warranty or guarantee offered by a third party, if any. All conditions, representations and warranties, whether express, implied, statutory or otherwise, including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, or non-infringement of third-party rights, are hereby disclaimed by all Parties to this Agreement to the maximum extent permitted by applicable law.

Survival. This Article VI shall survive any termination, cancellation, withdrawal or expiration of this Agreement.

VII. **NOTICE**

Any and all notices to be given under this Agreement by a State Agency shall be deemed to have been given if reduced to writing and delivered in person or mailed by overnight or certified mail, return receipt requested, postage pre-paid, to the Parties at the addresses set forth on the signatory pages below or to such other addresses designated in writing to all the State Agency. Any notice required hereunder shall be deemed to have been given three (3) days subsequent to the date it was so delivered or mailed.

VIII.

AMENDMENT

This Agreement may not be amended except in a written instrument specifically referring to this Agreement and signed by the Parties hereto. Any modification, alteration, addition or deletion to the terms of this Agreement which are required by changes in federal or state law are automatically incorporated herein without written amendment to this Agreement and shall be effective on the date designated by said law. In the event a Party becomes aware of any applicable change(s) in federal or state law, it will timely notify the other Party.

IX.

CURRENT REVENUE

The Parties hereby warrant that all payments, expenditures, contributions, fees, costs, and disbursements required of each Party hereunder or required by any other agreements, contracts and documents executed, adopted, or approved pursuant to this Agreement, which shall include any exhibit, attachment, addendum or associated document, shall be paid from current revenues and resources available to each paying Party. The Parties hereby warrant that no debt is created by this Agreement.

X.

FISCAL FUNDING

The obligations of the State Agency pursuant to this Agreement are contingent upon the availability and appropriation of sufficient funding. Any Party may withdraw from this Agreement without penalty in the event funds are not available or appropriated by giving the appropriate notice pursuant to Sections V and VII. However, no Party will be entitled to a refund of amounts previously contributed in the event of withdrawal for lack of funding, unless expressly agreed in writing by the Parties.

XI.

APPLICABLE LAW

This Agreement shall be expressly subject to the participating Parties' sovereign immunity and other governmental immunity and all applicable federal and state law. This Agreement shall be governed by and construed in accordance with the laws of the State of Texas. Venue shall lie exclusively in Tarrant County, Texas.

XII.

SEVERABILITY

In the event that one or more of the provisions contained in the Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability of the Agreement shall be construed as if such invalid, illegal or unenforceable

provision has never been contained herein, but shall not affect the remaining provisions of this Agreement, which shall remain in force and effect.

XIII. ASSIGNMENT

The Parties may not assign their respective rights and duties under this Agreement without the prior written consent and/or approval of the other Party acting by and through their respective governing bodies, even if such assignment is due to a change in ownership or affiliation. Any assignment attempted without such prior consent and/or approval by the other Party shall be null and void.

Survival. This Article XIII shall survive any termination, cancellation, withdrawal, or expiration of this Agreement.

XIV. ENTIRE AGREEMENT

This Agreement, including any and all exhibits, attachments, and/or addendums incorporated as a part hereof, shall constitute the entire agreement relating to the subject matter herein between the Parties and supersedes any other agreement concerning the subject matter of this transaction, whether oral or written. Each Party acknowledges that the other Parties, or anyone acting on behalf of the other Parties, have made no representations, inducements, promises or agreements, orally or otherwise, unless such representations, inducements, promises or agreements are embodied in this Agreement, expressly or by incorporation.

XV. RESPONSIBILITIES

All Parties agree to be responsible for their own negligent acts or omissions, or other tortious conduct in the course of performance of this Agreement without waiving any sovereign immunity, governmental immunity or other defenses available to the Parties under federal or state law. Nothing in this paragraph shall be construed to create or grant any rights, contractual or otherwise, in or to any third persons or entities. All Parties agree that any such liability or damages occurring during the performance of this Agreement caused by the joint or comparative negligence of the Parties, or their employees, agents or officers, shall be determined in accordance with comparative responsibility laws of Texas.

XVI. CJIS COMPLIANCE

All Parties and their respective employees, agents, contractors, and subcontractors agree, warrant, and represent they shall be compliant with the then current Federal Bureau of Investigations

Criminal Justice Information Security Policy, attached herein as EXHIBIT B, pursuant to this Agreement. Further, all Parties agree, warrant, and represent they are compliant with the Texas Department of Public Safety policies regarding access to Criminal Justice Information (CJI). Additionally, all Parties specifically agree to be responsible for their own individual ongoing compliance with regard to the Federal Bureau of Investigations Criminal Justice Information Security Policy and the Texas Department of Public Safety Criminal Justice Information policies.

XVII.

SOVEREIGN IMMUNITY

This Agreement is subject to Tarrant County's Sovereign Immunity and Tarrant County expressly does not waive any applicable local, State and federal rules and laws, including Sovereign Immunity, Title 5 of the Texas Civil Practice and Remedies Code. Further, the Parties acknowledge and agree Tarrant County does not have the ability under Article III, Section 49 and Article XI, Section 7 of the Texas Constitution to indemnify any party or third-party damages pursuant to this Agreement.

This Agreement is subject to State Agency's sovereign immunity as set forth in the Texas Civil Practice and Remedies Code. Further, the Parties acknowledge and agree State Agency does not have the ability under Article III, Sections 49, 50, 51, 55 or other applicable provisions of the Texas Constitution to indemnify any party or third-party damages pursuant to this Agreement.

[SIGNATORY PAGES SHALL FOLLOW]

BINDING AGREEMENT, AUTHORITY, PARTIES BOUND

By signing this page, each State Agency or Party represents that it has the full right, power and authority to enter and perform this MOU/ILA Among State Agencies and Tarrant County Criminal District Attorney for access to TechShare.Prosecutor via the TechShare.LEA Portal and in accordance with all of the terms and conditions, and that the execution and delivery of this Agreement has been made by an authorized representative of each Party to validly and legally bind the same Party to all terms, performances and provisions set forth in this Agreement.

SIGNED AND EXECUTED this ____ day of _____ 2024.

COUNTY OF TARRANT
STATE OF TEXAS

Separate Electronic Signature Page

Tim O'Hare
County Judge

John Hall, Vice President
University of Texas at Arlington Police Department

APPROVED AS TO FORM:



Criminal District Attorney's Office*

*By law, the Criminal District Attorney's Office may only approve contracts for its clients. We reviewed this document as to form from our client's legal perspective. Other parties may not rely on this approval. Instead, those parties should seek contract review from independent counsel.

SIGNATORY PAGE

BINDING AGREEMENT, AUTHORITY, PARTIES BOUND

By signing this page, each State Agency or Party represents that it has the full right, power and authority to enter and perform this MOU/ILA Among State Agencies and Tarrant County Criminal District Attorney for access to TechShare.Prosecutor via the TechShare.LEA Portal and in accordance with all of the terms and conditions, and that the execution and delivery of this MOU/ILA has been made by an authorized representative of each Party to validly and legally bind the same Party to all terms, performances and provisions set forth in this MOU/ILA.

The University of Texas at Arlington Police Department acknowledges that it is a "governmental entity" and not a "business entity" as those terms are defined in Tex. Gov't Code § 2252.908, and therefore, no disclosure of interested parties pursuant to Tex. Gov't Code §2252.908 is required.

UNIVERSITY OF TEXAS AT ARLINGTON POLICE DEPARTMENT ARLINGTON, TARRANT COUNTY, TEXAS

BY: _____
KIM LEMAUX

DATE: _____

Name: Kim Lemaux

Title: Chief of Police

Address: 202 E. Border St.

Arlington, Texas 76010

BY: _____
JOHN HALL, VICE PRESIDENT

DATE: _____

SIGNATORY PAGE

GENERAL SECURITY AND ACCESS OF DATA PROCEDURES

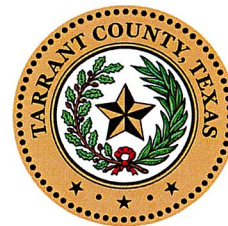
The following list serves as minimum requirements for the security and access of CJI in TSP via the LEA Portal pursuant to this MOU/ILA by the State Agency's Law Enforcement Agency (hereinafter "LEA").

- Each LEA must actively take responsibility for the management and the security of its Data. Data sharing via the LEA Portal will depend on adhering to professional standards, integrity, communication, and cooperation.
- Each LEA must ensure, prior to requesting LEA Portal access from TCDA for any user, that said user has passed the appropriate background screening requirements as mandated by the Texas Department of Public Safety.
- Each LEA must establish review and approval procedures for Data relating to Incidents, Arrests and Offenses submitted to TSP via the LEA Portal to ensure accuracy and consistency.
- Each LEA must ensure that all LEA users are aware that DME containing child pornography or other unlawful material is NOT to be uploaded into TSP via the LEA Portal, but shall be provided to TCDA via an external USB device.
- Each LEA is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines utilizing TSP and/or the LEA Portal, technical security to protect against unauthorized use of the LEA Portal, security of Data submitted through the LEA Portal, and dissemination of the Data not contained within TSP or the LEA Portal.
- Each LEA is responsible for the installation and maintenance of its interfaces to the LEA Portal and for securing (256 bit encrypted or more) communications to TSP via the LEA Portal.
- Each LEA shall designate at least one (1) authorized user to serve as the LEA Portal Administrator to establish review and approval procedures for its user access. The Administrator shall:
 - Act as primary contact to the CDA TSP Administrator and/or Tarrant County IT Customer Care on access problems and/or application issues.
 - Submit all user access requests to the Tarrant County IT Customer Care Center, on new users' behalf, via email at ITCustomerCare@tarrantcountytx.gov utilizing the Access Request Form ("ARF"), attached herein.

- Maintain a current list of authorized individual users and their Roles and permissions.
- Immediately cancel a user's access to the LEA Portal when the user is no longer associated with the LEA or is placed on administrative leave, by contacting the CDA TSP Administrator via email at LEAPortalHelp@tarrantcountytx.gov.
- Ensure that any Public Integrity incidents in the LEA Portal are flagged as Restricted so that only the detective assigned and the Point of Contact can access said incident.
- Register LEA users for TSP Training as it becomes available by TCDA for the proper protocol and use of the LEA Portal to submit criminal cases in TSP.
- Report any suspected unauthorized access and/or abuse by any LEA users to the CDA TSP Administrator as soon as possible.

ACCESS REQUEST FORM

Tarrant County Information Technology
200 N. Taylor St.
Fort Worth, TX 76196
Form: ARF01



User Requesting Access

Full Name:

Last

First

M.I.

Agency/Department: _____ Employee ID: _____

Position Title: _____

Business Address: _____

City

State

ZIP Code

Phone: _____

Email: _____

Will the user work remote? ☐ Yes ☐ No

If so, full address requested: _____

Person Authorizing Access (Authorizing Authority)

Authorized Approver Name: _____

Position Title: _____

Phone: _____

Email: _____

All forms must be emailed to ITCustomerCare@tarrantcountytx.gov from the authorized approver's email address. Email address and approver information MUST match.

Type of Request	Type of Access	TechShare Only	Type of User (Non-Tarrant County Employees)
☐ New Account	☐ Active Directory (TC Network)*	☐ Bond	☐ Temporary or Intern
☐ Update Account	☐ Email (TC email address)	☐ Case	☐ Consultant or Vendor
☐ Revoke Account	☐ TechShare (view TechShare column to specify)	☐ Clerk	☐ Law Enforcement
	☐ Cert (VPN access)	☐ Court	☐ Medical Examiner
	☐ Other _____	☐ Indigent Defense	☐ Federal, State, Local
		☐ Jail	☐ Other _____
		☐ Judicial Portal	☐ Contractor (Wireless M)
		☐ Juvenile	
		☐ LEA	
		☐ Magistrate	
		☐ Prosecutor	
		☐ Warrant	

Estimated Expiration Date: (if applicable): _____

ACCESS REQUEST FORM

Tarrant County Information Technology
200 N. Taylor St.
Fort Worth, TX 76196
Form: ARF01



If possible, please provide another account to mirror: _____

****A CJIS background check **MUST** be completed for all data access requests***

Justification (Please provide a brief description of why access is needed)

CJIS Requirements

A CJIS background check **MUST** be completed for all data access requests

For more information about CJIS requirements, go to <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>.

For questions about CJIS background checks, please contact the Tarrant County Customer Care Center at (817) 884-3507 or ITCustomerCare@tarrantcountytx.gov.

Has a CJIS background check been completed? ☐ Yes ☐ No

If applicable:

PID# _____

Police Identification Number

BAR# _____

Attorney Bar Number

Acknowledgement

I understand that I am requesting access to the Tarrant County Government network. It is for authorized business purposes only and governed by Tarrant County policies. Use of this system constitutes consent to security monitoring and testing. I also understand that I am responsible for the use and protection of the user ID and password that I will be provided.

Signature of Requestor: _____

Date: _____

Approval

I have verified that the information provided on the Access Request Form is correct and certify that the individual is authorized to receive the requested access.

Signature of Authorized Approver: _____ Date: _____

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including - but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI **ENS** Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to **en** shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI **ENS** systems and services to which the agency will have access, and the FBI **ENS** Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the **en**. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The **ENS** Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the **ENS** Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors

who perform criminal justice functions shall acknowledge, via signing of the **ens** Security Addendum Certification page, and abide by all aspects of the **ens** Security Addendum. The **ens** Security Addendum is presented in Appendix H. Modifications to the **ens** Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to **en**. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the **ens** Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to **en**. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the **ens** Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to **en**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to **en** shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to **en**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to **en** shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing **en** shall be subject to all pertinent areas of the **ens** Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI **en** shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to **en**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing **en** shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 - Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

CO# 144469



**COMMISSIONERS COURT
COMMUNICATION**

COURT ORDER NUMBER

PAGE 1 OF

DATE:

19

12/17/2024

**SUBJECT: CONSIDERATION OF A MEMORANDUM OF
UNDERSTANDING/INTERLOCAL AGREEMENT BETWEEN TARRANT
COUNTY CRIMINAL DISTRICT ATTORNEY AND STATE AGENCIES
FOR THE PARTICIPATION OF INFORMATION SHARING VIA
TECHSHARE.LEA AND TECHSHARE.PROSECUTOR**

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED

It is requested that the Commissioners Court consider a Memorandum of Understanding (MOU)/Interlocal Agreement (ILA) between Tarrant County Criminal District Attorney (CDA) and State Agencies for the participation of information sharing via TechShare.LEA and TechShare Prosecutor.

BACKGROUND

Since 2013, Tarrant County has been a participant in the TechShare Program. The Tarrant County CDA's Office uses the Techshare.Prosecutor system as its case management software in criminal cases. Law enforcement agencies utilize the Techshare.LEA portal to submit cases and evidence to the Criminal District Attorney's Office for prosecution.

This MOA/ILA memorializes the expectations and guidelines for the use of the data contained in TechShare between the CDA's Office and the University of Texas at Arlington Police Department ("UTAPD"). This agreement was requested by UTAPD as part of its certification process with the Texas Department of Public Safety.

With approval, the CDA's Office will continue to use the Techshare.Prosecutor system and continue to accept cases, data, and evidence submitted by UTAPD through Techshare.LEA.

The terms and conditions of this Agreement shall be indefinite unless terminated by one of the Parties.

The Criminal District Attorney's Office has approved this MOU/ILA as to form.

FISCAL IMPACT

There is no fiscal impact associated with this request.

SUBMITTED BY	Criminal District Attorney	PREPARED BY:	Polly Maxwell
		APPROVED BY:	Mark Kratovil

**MEMORANDUM OF UNDERSTANDING / INTERLOCAL AGREEMENT
WITH STATE AGENCIES AND TARRANT COUNTY CRIMINAL
DISTRICT ATTORNEY
TO PARTICIPATE IN INFORMATION SHARING VIA
TECHSHARE.LEA AND TECHSHARE.PROSECUTOR**

**I.
PARTIES**

This Memorandum of Understanding / Interlocal Agreement ("MOU/ILA") is entered by and between the undersigned State Agency of the State of Texas ("State Agency(s)"), acting by and through their respective Law Enforcement Agencies, pursuant to and under authority of the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code and for the purpose of sharing Criminal Justice Information ("CJI") via TechShare.LEA Portal ("LEA Portal") and TechShare.Prosecutor ("TSP") Applications. The undersigned State Agency / Law Enforcement Agency enters into this Interlocal Agreement ("Agreement") with Tarrant County Criminal District Attorney ("TCDA"). Any and all State Agencies of the State of Texas adopting this Agreement upon a formal order of their respective governing bodies as provided for herein may be referred to in this Agreement individually as "Party" and collectively as "Parties."

**II.
RECITALS**

WHEREAS, State Agency desire to enter into this Agreement to participate in the use of the LEA Portal to electronically file criminal cases with TCDA in TSP;

WHEREAS, State Agency will have access to the LEA Portal in order to file cases electronically, upload digital media evidence, search and share CJI, and perform other functions as allowed by statutes and role based permissions;

WHEREAS, TCDA agrees to provide access to the LEA Portal at no cost to State Agency and their designated Law Enforcement Agency personnel, and all Parties agree to abide by the terms and conditions laid out in this Agreement;

NOW THEREFORE, in consideration of the promises, inducements, covenants, agreements, conditions, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the State Agency and TCDA agree as follows:

III.

PARTICIPATION BY ADDITIONAL STATE AGENCIES

Any local government may participate in this Agreement with the signature of the designated authorized signer on the signatory page of this Agreement. Each State Agency will be required to approve and agree to the terms and conditions of this Agreement.

IV.

DATA OWNERSHIP, ACCESS, SECURITY AND STORAGE

- A. Ownership. TCDA owns the TechShare.Prosecutor and TechShare.LEA Portal software applications and has agreed to allow access to State Agency's LEA users. It is the intention of the Parties that each State Agency will remain the custodian and owner of its information and data that it created or submitted to TSP via the LEA Portal, unless expressly agreed in writing otherwise. The Parties acknowledge and agree that such information or data shall not be used by the Parties other than in connection with the performance of this Agreement or as contemplated by the Parties under this Agreement. Additionally, the Parties agree that the data shall not be disclosed, sold, assigned, leased or otherwise provided to third parties, or commercially exploited by or on behalf of the other Parties, their employees, officers, agents, subcontractors, invitees, or assigns in any respect without the expressed written approval of the State Agency that owns such data.
- B. Interfaces. Each Party is responsible for developing and maintaining its interfaces to the LEA Portal. State Agency is responsible for the cost of its own interface development and maintenance.
- C. Security and Access of Data.
- 1) Each Party is responsible for ensuring its employees and other persons accessing data within TSP via the LEA Portal are authorized to do so and will use such data only as is legally permitted, and as outlined in EXHIBIT A, attached herein.
 - 2) State Agency and their representatives agree that the following terms and conditions apply regarding access to the criminal justice information ("CJI") and data maintained in TSP:
 - a) State Agency and their representatives shall acknowledge and agree that the purpose of access to criminal justice information in the LEA Portal is to perform criminal justice related functions.

- b) State Agency agrees that the LEA Portal shall not be used for any personal purposes, including entertainment, personal business, or personal gain.
- c) State Agency understands that access to, and transmission of, any data or material deemed to be a violation of any federal, state, or local law or agency administrative rules is prohibited.

Survival. This Article IV shall survive any termination, cancellation, withdrawal, or expiration of this Agreement.

V. **TERMS AND TERMINATION**

The terms and conditions of this Agreement shall be indefinite unless terminated by one of the Parties. This Agreement may be terminated by either Party with a thirty (30) day written notice to the other Party.

VI. **WARRANTIES**

No Party to this Agreement warrants the availability, accuracy, quality, reliability or fitness for a particular purpose of any data or information made available under this Agreement. Third party warranties or guarantees may inure to the benefit of the Parties to a particular Project if such are contractually secured as apart of such Project; however, no Party to this Agreement shall be held liable for a warranty or guarantee offered by a third party, if any. All conditions, representations and warranties, whether express, implied, statutory or otherwise, including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, or non-infringement of third-party rights, are hereby disclaimed by all Parties to this Agreement to the maximum extent permitted by applicable law.

Survival. This Article VI shall survive any termination, cancellation, withdrawal or expiration of this Agreement.

VII. **NOTICE**

Any and all notices to be given under this Agreement by a State Agency shall be deemed to have been given if reduced to writing and delivered in person or mailed by overnight or certified mail, return receipt requested, postage pre-paid, to the Parties at the addresses set forth on the signatory pages below or to such other addresses designated in writing to all the State Agency. Any notice required hereunder shall be deemed to have been given three (3) days subsequent to the date it was so delivered or mailed.

VIII.
AMENDMENT

This Agreement may not be amended except in a written instrument specifically referring to this Agreement and signed by the Parties hereto. Any modification, alteration, addition or deletion to the terms of this Agreement which are required by changes in federal or state law are automatically incorporated herein without written amendment to this Agreement and shall be effective on the date designated by said law. In the event a Party becomes aware of any applicable change(s) in federal or state law, it will timely notify the other Party.

IX.
CURRENT REVENUE

The Parties hereby warrant that all payments, expenditures, contributions, fees, costs, and disbursements required of each Party hereunder or required by any other agreements, contracts and documents executed, adopted, or approved pursuant to this Agreement, which shall include any exhibit, attachment, addendum or associated document, shall be paid from current revenues and resources available to each paying Party. The Parties hereby warrant that no debt is created by this Agreement.

X.
FISCAL FUNDING

The obligations of the State Agency pursuant to this Agreement are contingent upon the availability and appropriation of sufficient funding. Any Party may withdraw from this Agreement without penalty in the event funds are not available or appropriated by giving the appropriate notice pursuant to Sections V and VII. However, no Party will be entitled to a refund of amounts previously contributed in the event of withdrawal for lack of funding, unless expressly agreed in writing by the Parties.

XI.
APPLICABLE LAW

This Agreement shall be expressly subject to the participating Parties' sovereign immunity and other governmental immunity and all applicable federal and state law. This Agreement shall be governed by and construed in accordance with the laws of the State of Texas. Venue shall lie exclusively in Tarrant County, Texas.

XII.
SEVERABILITY

In the event that one or more of the provisions contained in the Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability of the Agreement shall be construed as if such invalid, illegal or unenforceable

provision has never been contained herein, but shall not affect the remaining provisions of this Agreement, which shall remain in force and effect.

XIII. ASSIGNMENT

The Parties may not assign their respective rights and duties under this Agreement without the prior written consent and/or approval of the other Party acting by and through their respective governing bodies, even if such assignment is due to a change in ownership or affiliation. Any assignment attempted without such prior consent and/or approval by the other Party shall be null and void.

Survival. This Article XIII shall survive any termination, cancellation, withdrawal, or expiration of this Agreement.

XIV. ENTIRE AGREEMENT

This Agreement, including any and all exhibits, attachments, and/or addendums incorporated as a part hereof, shall constitute the entire agreement relating to the subject matter herein between the Parties and supersedes any other agreement concerning the subject matter of this transaction, whether oral or written. Each Party acknowledges that the other Parties, or anyone acting on behalf of the other Parties, have made no representations, inducements, promises or agreements, orally or otherwise, unless such representations, inducements, promises or agreements are embodied in this Agreement, expressly or by incorporation.

XV. RESPONSIBILITIES

All Parties agree to be responsible for their own negligent acts or omissions, or other tortious conduct in the course of performance of this Agreement without waiving any sovereign immunity, governmental immunity or other defenses available to the Parties under federal or state law. Nothing in this paragraph shall be construed to create or grant any rights, contractual or otherwise, in or to any third persons or entities. All Parties agree that any such liability or damages occurring during the performance of this Agreement caused by the joint or comparative negligence of the Parties, or their employees, agents or officers, shall be determined in accordance with comparative responsibility laws of Texas.

XVI. CJIS COMPLIANCE

All Parties and their respective employees, agents, contractors, and subcontractors agree, warrant, and represent they shall be compliant with the then current Federal Bureau of Investigations

Criminal Justice Information Security Policy, attached herein as EXHIBIT B, pursuant to this Agreement. Further, all Parties agree, warrant, and represent they are compliant with the Texas Department of Public Safety policies regarding access to Criminal Justice Information (CJI). Additionally, all Parties specifically agree to be responsible for their own individual ongoing compliance with regard to the Federal Bureau of Investigations Criminal Justice Information Security Policy and the Texas Department of Public Safety Criminal Justice Information policies.

XVII.
SOVEREIGN IMMUNITY

This Agreement is subject to Tarrant County's Sovereign Immunity and Tarrant County expressly does not waive any applicable local, State and federal rules and laws, including Sovereign Immunity, Title 5 of the Texas Civil Practice and Remedies Code. Further, the Parties acknowledge and agree Tarrant County does not have the ability under Article III, Section 49 and Article XI, Section 7 of the Texas Constitution to indemnify any party or third-party damages pursuant to this Agreement.

This Agreement is subject to State Agency's sovereign immunity as set forth in the Texas Civil Practice and Remedies Code. Further, the Parties acknowledge and agree State Agency does not have the ability under Article III, Sections 49, 50, 51, 55 or other applicable provisions of the Texas Constitution to indemnify any party or third-party damages pursuant to this Agreement.

[SIGNATORY PAGES SHALL FOLLOW]

BINDING AGREEMENT, AUTHORITY, PARTIES BOUND

By signing this page, each State Agency or Party represents that it has the full right, power and authority to enter and perform this MOU/ILA Among State Agencies and Tarrant County Criminal District Attorney for access to TechShare.Prosecutor via the TechShare.LEA Portal and in accordance with all of the terms and conditions, and that the execution and delivery of this Agreement has been made by an authorized representative of each Party to validly and legally bind the same Party to all terms, performances and provisions set forth in this Agreement.

SIGNED AND EXECUTED this ____ day of _____ 2024.

COUNTY OF TARRANT
STATE OF TEXAS

Separate Electronic Signature Page

Tim O'Hare
County Judge

John Hall, Vice President
University of Texas at Arlington Police Department

APPROVED AS TO FORM:



Criminal District Attorney's Office*

*By law, the Criminal District Attorney's Office may only approve contracts for its clients. We reviewed this document as to form from our client's legal perspective. Other parties may not rely on this approval. Instead, those parties should seek contract review from independent counsel.

SIGNATORY PAGE

BINDING AGREEMENT. AUTHORITY, PARTIES BOUND

By signing this page, each State Agency or Party represents that it has the full right, power and authority to enter and perform this MOU/ILA Among State Agencies and Tarrant County Criminal District Attorney for access to TechShare.Prosecutor via the TechShare.LEA Portal and in accordance with all of the terms and conditions, and that the execution and delivery of this MOU/ILA has been made by an authorized representative of each Party to validly and legally bind the same Party to all terms, performances and provisions set forth in this MOU/ILA.

The University of Texas at Arlington Police Department acknowledges that it is a "governmental entity" and not a "business entity" as those terms are defined in Tex. Gov't Code § 2252.908, and therefore, no disclosure of interested parties pursuant to Tex. Gov't Code §2252.908 is required.

**UNIVERSITY OF TEXAS AT ARLINGTON POLICE DEPARTMENT
ARLINGTON, TARRANT COUNTY, TEXAS**

BY: _____
KIM LEMAUX

DATE: _____

Name: Kim Lemaux

Title: Chief of Police

Address: 202 E. Border St.

Arlington, Texas 76010

BY: _____
JOHN HALL, VICE PRESIDENT

DATE: _____

SIGNATORY PAGE

Page | 8

MEMORANDUM OF UNDERSTANDING / INTERLOCAL AGREEMENT

GENERAL SECURITY AND ACCESS OF DATA PROCEDURES

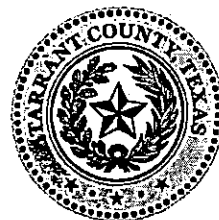
The following list serves as minimum requirements for the security and access of CJI in TSP via the LEA Portal pursuant to this MOU/ILA by the State Agency's Law Enforcement Agency (hereinafter "LEA").

- Each LEA must actively take responsibility for the management and the security of its Data. Data sharing via the LEA Portal will depend on adhering to professional standards, integrity, communication, and cooperation.
- Each LEA must ensure, prior to requesting LEA Portal access from TCDA for any user, that said user has passed the appropriate background screening requirements as mandated by the Texas Department of Public Safety.
- Each LEA must establish review and approval procedures for Data relating to Incidents, Arrests and Offenses submitted to TSP via the LEA Portal to ensure accuracy and consistency.
- Each LEA must ensure that all LEA users are aware that DME containing child pornography or other unlawful material is NOT to be uploaded into TSP via the LEA Portal, but shall be provided to TCDA via an external USB device.
- Each LEA is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines utilizing TSP and/or the LEA Portal, technical security to protect against unauthorized use of the LEA Portal, security of Data submitted through the LEA Portal, and dissemination of the Data not contained within TSP or the LEA Portal.
- Each LEA is responsible for the installation and maintenance of its interfaces to the LEA Portal and for securing (256 bit encrypted or more) communications to TSP via the LEA Portal.
- Each LEA shall designate at least one (1) authorized user to serve as the LEA Portal Administrator to establish review and approval procedures for its user access. The Administrator shall:
 - Act as primary contact to the CDA TSP Administrator and/or Tarrant County IT Customer Care on access problems and/or application issues.
 - Submit all user access requests to the Tarrant County IT Customer Care Center, on new users' behalf, via email at ITCustomerCare@tarrantcountytx.gov utilizing the Access Request Form ("ARF"), attached herein.

- Maintain a current list of authorized individual users and their Roles and permissions.
- Immediately cancel a user's access to the LEA Portal when the user is no longer associated with the LEA or is placed on administrative leave, by contacting the CDA TSP Administrator via email at LEAPortalHelp@tarrantcountytx.gov.
- Ensure that any Public Integrity incidents in the LEA Portal are flagged as Restricted so that only the detective assigned and the Point of Contact can access said incident.
- Register LEA users for TSP Training as it becomes available by TCDA for the proper protocol and use of the LEA Portal to submit criminal cases in TSP.
- Report any suspected unauthorized access and/or abuse by any LEA users to the CDA TSP Administrator as soon as possible.

ACCESS REQUEST FORM

Tarrant County Information Technology
200 N. Taylor St.
Fort Worth, TX 76196
Form: ARF01



User Requesting Access

Full Name:

Last First M.I.

Agency/Department: _____ Employee ID: _____

Position Title: _____

Business Address: _____

City State ZIP Code

Phone: _____ Email: _____

Will the user work remote? ☐ Yes ☐ No

If so, full address requested: _____

Person Authorizing Access (Authorizing Authority)

Authorized Approver Name: _____

Position Title: _____

Phone: _____ Email: _____

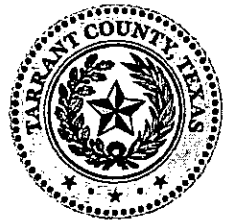
All forms must be emailed to ITCustomerCare@tarrantcountytx.gov from the authorized approver's email address. Email address and approver information MUST match.

Type of Request	Type of Access	TechShare Only	Type of User (Non-Tarrant County Employees)
☐ New Account	☐ Active Directory (TC Network)*	☐ Bond	☐ Temporary or Intern
☐ Update Account	☐ Email (TC email address)	☐ Case	☐ Consultant or Vendor
☐ Revoke Account	☐ TechShare (view TechShare column to specify)	☐ Clerk	☐ Law Enforcement
	☐ Cert (VPN access)	☐ Court	☐ Medical Examiner
	☐ Other _____	☐ Indigent Defense	☐ Federal, State, Local
		☐ Jail	☐ Other _____
		☐ Judicial Portal	☐ Contractor (Wireless M)
		☐ Juvenile	
		☐ LEA	
		☐ Magistrate	
		☐ Prosecutor	
		☐ Warrant	

Estimated Expiration Date: (if applicable): _____

ACCESS REQUEST FORM

Tarrant County Information Technology
200 N. Taylor St.
Fort Worth, TX 76196
Form: ARF01



If possible, please provide another account to mirror: _____

****A CJIS background check MUST be completed for all data access requests***

Justification (Please provide a brief description of why access is needed)

CJIS Requirements

A CJIS background check MUST be completed for all data access requests

For more information about CJIS requirements, go to <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center>.

For questions about CJIS background checks, please contact the Tarrant County Customer Care Center at (817) 884-3507 or ITCustomerCare@tarrantcountytx.gov.

Has a CJIS background check been completed? ☐ Yes ☐ No

If applicable:

PID# _____

Police Identification Number

BAR# _____

Attorney Bar Number

Acknowledgement

I understand that I am requesting access to the Tarrant County Government network. It is for authorized business purposes only and governed by Tarrant County policies. Use of this system constitutes consent to security monitoring and testing. I also understand that I am responsible for the use and protection of the user ID and password that I will be provided.

Signature of Requestor: _____

Date: _____

Approval

I have verified that the information provided on the Access Request Form is correct and certify that the individual is authorized to receive the requested access.

Signature of Authorized Approver: _____ Date: _____

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including - but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI ENS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to EN shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI ENS systems and services to which the agency will have access, and the FBI ENS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the EN. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The ENS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the ENS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors

who perform criminal justice functions shall acknowledge, via signing of the **ENS** Security Addendum Certification page, and abide by all aspects of the **ENS** Security Addendum. The **ENS** Security Addendum is presented in Appendix H. Modifications to the **ENS** Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to **EN**. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the **ENS** Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to **EN**. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the **ENS** Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to **EN**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to **EN** shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to **EN**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to **EN** shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing **EN** shall be subject to all pertinent areas of the **ENS** Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI **EN** shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to **EN**. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing **EN** shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

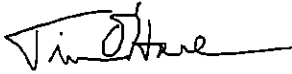
Figure 3 - Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

Consideration of a Memorandum of Understanding/Interlocal Agreement between Tarrant
County Criminal District Attorney and Participating Local Governments for the Participation of
Information Sharing Via TechShare.LEA and TechShare.Prosecutor

SIGNED AND EXECUTED this 17 day of December, 2024.

**COUNTY OF TARRANT
STATE OF TEXAS**

A handwritten signature in black ink, appearing to read "Tim O'Hare", with a long horizontal flourish extending to the right.

Tim O'Hare
County Judge
12/19/2024