

TechShare Local Government Corporation

TechShare.Magistration Public Safety Assessment Tool Development and Implementation Agreement

1. Background and Purpose

- 1.1. Tarrant County is a participant in the Master Interlocal Agreement for Stakeholder Participation in TechShare and is a Stakeholder sharing the TechShare.Magistration resource.
- 1.2. Tarrant County has requested the development of the Public Safety Assessment Tool in TechShare.Magistration
- 1.3. This Agreement is entered into by and between the TechShare Local Government Corporation ("TechShare") and Tarrant County for the purpose of developing and implementing the TechShare.Magistration Public Safety Assessment Tool in Tarrant County.

2. Term of Agreement

- 2.1. This Agreement shall be effective from upon approval of this agreement by the Tarrant County Commissioners Court and shall remain effective through the completion of the scope of work as set forth in Attachment A.

3. Project Approach, Staffing, Deliverables and Budget

- 3.1. The Project Approach, Staffing, Deliverables and Budget are included as Attachment A.

4. Compensation of TechShare

- 4.1. TechShare shall be compensated as set forth in Attachment A.
- 4.2. TechShare will invoice Tarrant County for the amounts indicated in Attachment A, Project Budget, as prescribed for each milestone. Payment is due from Tarrant County no later than thirty days after invoice date. TechShare cannot begin work until payment is received for the first milestone.
- 4.3. Since the Public Safety Assessment Tool functionality that will be added TechShare.Magistration will be shared by other participating counties, TechShare will prepare and present to the Magistration Stakeholder Committee a request to add the total cost of the project to the total capital value of TechShare.Magistration and Tarrant County's share in the total capital value.

5. Miscellaneous

- 5.1. This Agreement may not be amended except in a written instrument specifically referring to this Agreement and signed by the Parties hereto.
- 5.2. Each Party represents that it has, as of the date of the execution of this Agreement, obtained all requisite approvals and authority to enter into and perform its obligations under this Agreement, including the funds necessary to satisfy its obligations herein.
- 5.3. In the event any term or provision of this Agreement conflicts with any provision of law or is declared to be invalid or illegal for any reason, this Agreement will remain in full force and effect and will be interpreted as though such invalid or illegal provision were not a part of this Agreement. The remaining provisions will be construed to preserve the intent and purpose of this Agreement and the Parties will

negotiate in good faith to modify any invalidated provisions to preserve each Party's anticipated benefits.

- 5.4. This instrument contains the entire agreement with respect to the development and implementation planning of the enhancements to TechShare.Magistration listed in Attachment A, between the parties relating to the rights granted and the obligations assumed. Any prior implementation agreements or representations not expressly set forth in this Agreement are of no force.
- 5.5. Tarrant County and TechShare agree that each is responsible for its own proportionate share of any liability for the negligent acts or omissions of its employees, agents, contractors, or subcontractors arising out of, connected with, or as a consequence of its performance under this Agreement. Neither party will be liable to the other for any indirect, special, incidental, punitive, or consequential damages, including for loss of business, revenue, profits, or other economic advantage. This is regardless of how the damage arises, whether in action of contract, negligence, tort, or other action, arising out of or in connection with this contract, even if advised of its possibility.
- 5.6. Entities that Boycott Israel and Prohibition against Involvement with Iran, Sudan, and Foreign Terrorist Organizations. In compliance with Texas Government Code Section 2252.152, if applicable, TechShare verifies that it does not boycott Israel and will not boycott Israel during the term of this Agreement. Further, TechShare further verifies that it is not engaged in business with Iran, Sudan, or any foreign terrorist organization. The term "foreign terrorist organization" means an organization designated as a foreign terrorist organization by the United States Secretary of State as authorized by 8 U.S.C. Section 1189.
- 5.7. Compliance with Laws. In providing the services required by this Agreement, TechShare must observe and comply with all applicable federal, state, and local statutes, ordinances, rules, and regulations, including, without limitation, workers' compensation laws, minimum and maximum salary and wage statutes and regulations, and non-discrimination laws and regulations. TechShare shall be responsible for ensuring its compliance with any laws and regulations applicable to its business, including maintaining any necessary licenses and permits.
- 5.8. Trade Associations. In compliance with Section 2274.002 of the Texas Government Code, if applicable, TechShare certifies it does not boycott energy companies and shall not boycott energy companies during the terms of this Agreement. "Boycott energy company" is defined in Section 809.001(1) and means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company: (A) engages in the exploration, production, utilization, transportation, sale, or manufacturing of fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; or (B) does business with a company described by subsection (A).
- 5.9. Discrimination against Firearm Entities or Firearm Trade Associations Prohibited. In compliance with Section 2274.002 of the Texas Government Code, if applicable, TechShare certifies that it does not have a practice, policy, guidance or directive that discriminates against a firearm entity or firearm trade association; and will not discriminate during the term of the above described contract] against a firearm entity or firearm trade association. "Discriminate against a firearm entity or firearm trade association" is defined in Section 2274.001(3) and means, with respect to the entity or association, to: (i) refuse to

engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (ii) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (iii) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; the term *does not include*: (i) the established policies of a merchant, retail seller, or platform that restrict or prohibit the listing or selling of ammunition, firearms, or firearm accessories; and (ii) a company's refusal to engage in the trade of any goods or services, decision to refrain from continuing an existing business relationship, or decision to terminate an existing business relationship: (aa) to comply with federal, state, or local law, policy, or regulations or a directive by a regulatory agency; or (bb) for any traditional business reason that is specific to the customer or potential customer and not based solely on an entity's or association's status as a firearm entity or firearm trade association.

6. Attachments Incorporated

- 6.1. Attachment A: Project Approach, Staffing, Deliverables and Budget are incorporated in this Agreement as if fully set forth herein.
- 6.2. Attachment B: Federal Bureau of Investigation Criminal Justice Information Services Security Addendum.

[Signature Page to Follow]

TARRANT COUNTY:

RECOMMENDED BY:

Tim O'Hare
Tarrant County Judge

TECHSHARE LOCAL GOVERNMENT CORPORATION

BY: _____

Title: Executive Director

Date: _____

Name and Address for Purposes of Notice:

G.K. Maenius
500 W. 13th Street
Austin, TX 78701

05012024

APPROVED AS TO FORM:

CERTIFICATION OF
AVAILABLE FUNDS: \$ _____

Kimberly Colliet Wesley
Criminal District Attorney's Office*

Tarrant County Auditor

*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.

Introduction

This document outlines the mutual understanding between TechShare LGC and Tarrant County regarding the scope, objectives, and deliverables of the Public Safety Assessment Tool for TechShare.Magistration Development and Implementation Project. The purpose of this SOW is to ensure clarity, alignment, and accountability throughout the project lifecycle, enabling both parties to effectively collaborate towards successful outcomes. By detailing the project's goals, milestones, timelines, and responsibilities, this document serves as a roadmap for execution and evaluation.

Throughout this SOW, you will find a comprehensive overview of the project's scope, including specific tasks, deliverables, acceptance criteria, and any relevant assumptions or constraints. Additionally, we have outlined the roles and responsibilities of each party involved, ensuring clear communication channels and accountability at every stage.

Our mutual commitment to transparency, communication, and excellence will be instrumental in achieving the desired results outlined in this document. We look forward to a productive partnership and the successful execution of the development and implementation of Public Safety Assessment Tool for TechShare.Magistration.

Scope of Work

The Public Safety Assessment (PSA) is a tool designed to predict the probability that individuals will attend their court appointments and refrain from engaging in illegal activities while on pretrial release. The PSA is designed to evaluate adults aged eighteen (18) or older who have been arrested, booked into jail, and are awaiting case disposition. The PSA is not intended for use with individuals charged while already incarcerated or for those found guilty and awaiting sentencing or appeal in the community.

The PSA is currently in use within Tarrant County through another service provider. Tarrant County would like to move to a county managed solution and has requested a quote from TechShare for services related to development and implementation of the Public Safety Assessment Tool for Tarrant County within the TechShare.Magistration portal.

Objectives

- Development of the Public Safety Assessment Tool within TechShare.Magistration
- Implementation of the Public Safety Assessment Tool

Software Requirements

The following table lists the identified software requirements for this project:

ID	Requirement
FR001	The PSA score must be calculated using only the nine PSA factors.

TechShare.Magistration
PUBLIC SAFETY ASSESSMENT TOOL
Attachment A
STATEMENT OF WORK
TARRANTCOUNTY

ID	Requirement
FR002	The PSA nine factors must not be altered.
FR003	The PSA point values must not be altered.
FR004	The PSA scaled scoring rules must not be altered.
FR005	The PSA's nine factors must be used to calculate three scores: Failure to Appear (FTA), New Criminal Arrest (NCA), and New Violent Criminal Arrest (NVCA).
FR006	FTA and NCA must be reported as a scaled score.
FR007	NVCA must be reported as the presence or absence of a flag.
FR008	Each score must be reported separately; do not combine them into one score
FR009	A user must be allowed to manually enter Out of County offenses to the defendant's Criminal History before the PSA scores are calculated.
FR010	Magistrate Support Officers (MSOs) or assessors must use an automated system to calculate PSA. Calculating the scores by hand is strictly prohibited
FR011	The person's results for each of the PSA's nine factors and their three scores must be included on each pretrial assessment report.
FR012	An ongoing quality assurance process must be implemented to ensure that the PSA is scored accurately and reported correctly.
FR013	The way the PSA is calculated must be easily accessible to be audited at any given time to ensure the adherence to the Arnold PSA formula.
DR001	Person name (required)
DR002	Person date of birth (required)
DR003	Person SID number (required)
DR004	Person address (optional)
DR005	Person phone number (optional)
DR006	Date of arrest (required)
DR007	Case number (optional)
DR008	SID number (required)
DR009	Most serious offense (aka primary offense) (required)
DR010	Other pending cases?
DR011	Number of FTAs in the last 2 years?
DR012	FTAs in cases older than 2 years?

TechShare.Magistration
PUBLIC SAFETY ASSESSMENT TOOL
Attachment A
STATEMENT OF WORK
TARRANTCOUNTY

ID	Requirement
DR013	Prior misdemeanor convictions?
DR014	Prior felony convictions?
DR015	Number of violent offense convictions?
DR016	Previously sentenced to jail/prison more than 14 days?
DR017	Data destruction or data purge must not occur until expressed written permission is received by the TechShare from Tarrant County, after which a written certification of data destruction will be required
TR001	All production data should be hosted in a government cloud certified environment in compliance with the International Traffic in Arms Regulations (ITAR), the Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Security Management Act (FISMA), Criminal Justice Information Services (CJIS), and the Health Insurance and Accountability Act (HIPAA).
TR002	The proposed solution must support the Role Based Access Control (RBAC)
TR003	The solution MUST be compatible with Tarrant County-preferred Internet browsers (Microsoft Edge, Chrome Enterprise, and/or Mozilla Firefox Extended Support Release) with minimal or no loss of functionality based on browser selected, when applicable
TR004	The solution should be able to integrate with TechShare Jail, TechShare Court, and TechShare Magistration portal.
TR005	The PSA application must support anytime, anywhere access to stored content. This includes strong encryption of data traffic while in transit and at rest, for sensitive data, when applicable.
TR006	The product should support County user single sign-on (SSO) capability facilitated through a hosted government cloud-certified environment.
TR007	TechShare must provide onsite “train the trainer” and/or remote end-user training options
RR001	Completed Assessment Report
RR002	Completed Assessment Report Raw Data
RR003	Frequency of Offenses Report
RR004	PSA Risk Profile Report
RR005	Risk Level Report
RR006	Stale Subjects Report
RR007	Tarrant PSA Raw Data
RR008	Utility – Integration – Subject Profiles EID Report
RR009	Utility – Possible Duplicate Subjects
DR01	Extract and all reports.

ID	Requirement
DR02	Remove all integrations to the Noble application.
DR03	Create a place to store reports for audit purposes

Quality Assurance Standards

Below describes the quality assurance services to be provided by the TechShare team to ensure the delivery of high-quality software which meets user expectations and performance requirements.

1. **Test Plan** Development of a comprehensive test plan and strategy which outlines the approach, scope, objectives, and resources for testing activities throughout the software development lifecycle.
2. **Development Testing** employed within the development team, TechShare utilizes unit testing and peer reviews to ensure the developed software has the quality, maintainability, and adherence to standards.
3. **Internal Quality Assurance** testing of the feature upon incorporation into a new build.
4. **Product Owner** testing as new builds are deployed to the project environment.
5. **Acceptance Testing** to validate the software meets the acceptance criteria defined by stakeholders and fulfills the business requirements to go live on the software.

Timeline/Schedule

The projected timeline for this project spans six (6) months. Specific tasks and their corresponding milestones are detailed in the table provided below, aligning with the established period for project completion. There are no anticipated adjustments to the time for this effort.

Task	1	2	3	4	5	6
	Kick Off	Develop	Develop	Develop & Test	Test & Train	Train & Go Live
Validate Requirements						
Status Reports						
Development of PSA						
Upgrade Integration Framework						
Environment and Application Configuration						
Test Plan						
Implementation Initiation						

TechShare.Magistration
PUBLIC SAFETY ASSESSMENT TOOL
Attachment A
STATEMENT OF WORK
TARRANTCOUNTY

Task	1	2	3	4	5	6
	Kick Off	Develop	Develop	Develop & Test	Test & Train	Train & Go Live
Training Plan						
User Acceptance Testing						
Training						
Go Live						

Roles and Responsibilities

The below **RACI** chart provides clarity on who is **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed for each task within this Statement of Work.

Project Task	TS Product Manager	TS Sr. Business Analyst	TS Developer	TS QA	TC Business Product Owner	TC Stakeholder	TC ITD
Product Management Services	R	I	I	I	I	I	I
Validate Requirements	R	A	I	I	C	I	I
Design and Architecture	R	I	A	I	I	I	I
Development	R	C	A	I	I	I	I
Integration Framework Upgrade	R	C	A	I	I	I	I
Configuration	R	A	C	I	I	I	C
Testing/QA	R	I	I	A	A	I	I
Deployment	A	I	I	I	I	I	R
Release Notes	R	R	I	I	I	I	I
Sprint Review	R	A	A	A	I	I	I
Change Management	R	I	I	I	I	A	A
Communication and Reporting	R/A	I	I	I	I	I	I

Project Task	TS Product Manager	TS Sr. Business Analyst	TS Developer	TS QA	TC Business Product Owner	TC Stakeholder	TC ITD
Test Plan	R	A	I	A	I	I	I
Training Plan	R	A	I	A	A	I	I
Implementation Plan	R	I	I	I	I	I	I
Implementation Readiness Sign Off	I	I	I	I	A	R	I
Go Live Sign Off	I	I	I	I	A	R	I
Knowledge Transfer	R	A	A	C	I	I	A
Post Go Live Activities	R	A	A	A	A	I	A

Change Management Process

By following a structured change management process, software development projects can effectively manage changes while minimizing disruptions and maintaining alignment with project goals. While there are no changes to the scope of work or timeline for this effort envisioned, should there be any, they will be managed collaboratively by TechShare and Tarrant County to develop a Change Request for review and approval by Stakeholders in advance of deviating from the original scope or timeline of this project.

Assumptions and Constraints

1. The Public Safety Assessment Tool will be developed as an enhancement to the existing TechShare.Magistration portal.
2. Development, Project Management, and Implementation Services are provided by TechShare.
3. Development meetings will be conducted by TechShare with designated Tarrant County business team members to complete development of the Public Safety Assessment Tool (on-site and remote.)
4. TechShare will provide application configuration services of the application in the Tarrant County environment.
5. TechShare will coordinate quality assurance and user acceptance testing activities.
6. Training will be provided by TechShare with options for in-person and remote sessions.

7. TechShare will provide transition information for Tarrant County including a review of the architecture with Tarrant County and a knowledge transfer session on how to access any artifacts of the project.

Acceptance Criteria

1. The system meets all functional requirements outlined in the project scope.
2. The system meets all non-functional requirements such as performance, reliability, security, usability, and scalability. This includes adequate response time, system up time, data security, and the user experience.
3. Documentation for training and use of the system.
4. Documentation for technical support of the system.

Deliverables

1. Weekly Status Report to include project updates, metrics regarding development, and implementation progress, costs, issues & risks, action Items, upcoming milestones, dependencies, and overall project health.
2. Working Software based on the requirements described in the Scope of Work.
3. Training Materials for Train the Trainer Sessions
4. Train the Trainer Sessions.
5. Test Plan for User Acceptance Testing.
6. Facilitation of User Acceptance Testing.
7. Technical Training for Tarrant County ITD and access to project artifacts for the development of the system.

Payment Terms

The total cost of this effort is \$185,040. The following describes the payment terms including the amount due based on the identified milestones:

No	Milestone	Amount	Payment Term
1	Development of Public Safety Assessment Tool for TechShare.Magistration	\$111,024	Sixty percent (60%) due upon signing of agreement and in advance of starting the project
2	Implementation of Public Safety Assessment Tool for TechShare.Magistration	\$55,512	Thirty percent (30%) due upon sign off for Implementation Readiness
3	Go Live Services	\$18,504	Ten percent (10%) due upon a go decision to proceed with go live of the system

Attachment B
FEDERAL BUREAU OF INVESTIGATION CRIMINAL
JUSTICE INFORMATION SERVICES SECURITY
ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

- 1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.
- 1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

- 2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

3.00 Responsibilities of the Contractor.

- 3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

- 4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

- 4.02 Security violations can justify termination of the appended agreement.
- 4.03 Upon notification, the FBI reserves the right to:
- a. Investigate or decline to investigate any report of unauthorized use;
 - b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

- 5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

- 6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
- 6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
- 6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- 6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.
- 6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division,
FBI 1000 Custer Hollow Road
Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Contractor

TechShare Local Government Corporation

Signature of Contract Representative

Date

G.K. Maenius, Executive Director

Printed Name and Title