CJIS Trusted Broker
Privileged User Application

WARNING

CJIS TB is an official U.S. Government system for authorized use only by authorized members of the law enforcement, criminal justice and public safety community. Information presented in this system is considered sensitive but not classified and is for official law enforcement/criminal justice/public safety use only. The use of this system will be monitored for security and administration purposes and accessing this system constitutes consent to such monitoring. Any unauthorized access of this system or unauthorized use of the information provided on the CJIS TB network is prohibited and may be subject to criminal and civil penalties under federal law.

This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

CJIS TB will collect and store system and network related information in a persistent cookie. The purpose of collecting and storing this information is so that CJIS TB can enhance its security by employing advanced authentication reliant on this information. The information is encrypted and CJIS TB will not share this with any unauthorized parties.

Warning! The use of publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access CJIS TB is unauthorized. This type of usage may result in the involuntary dissemination of information to unauthorized entities. Data may be left on this computer resulting in the next person using this machine the ability to view your data.

PRIVACY ACT STATEMENT

General - This information is provided pursuant to Public Law 93-579 (Privacy Act of 1974) for individuals completing CJIS TB user application forms. Authority - CJIS TB is a federally funded national communications system established by the FBI. Application information is solicited under the authority of the Federal Records Act (Title 44, United States Code) and implementing regulations (Title 36, Code of Federal Regulations, chapter XII). Purpose and Use - The principal purposes of CJIS TB user application forms are to collect information needed to determine qualifying factors for authorized use, and verification of identity. This completed application will be used to register this account as a qualified CJIS TB account. All or part of the submitted information may be disclosed outside the FBI to federal, state, local, or tribal law enforcement agencies charged with the responsibility of investigating a violation or potential violation of the law and to applicant agency or organization to periodically verify continued access to CJIS TB. Disclosure may otherwise be made pursuant to the routine uses most recently published in the Federal Register for the FBI's Central Records System (Justice/FBI 002). Failure to provide the requested information shall result in the denial of this application.

Instructions: Type or write the information requested. **ALL FIELDS ARE MANDATORY.** Fax, mail, or e-mail the completed application to the information located in the upper right hand portion of page one of this form. **Send all pages, including a signed FD-889a Rules of Behavior form.** IMPORTANT: Non-legible applications will not be processed

1. Applicant Information

Applicant Name (Last, First, MI) :

Title / Position:
(do not abbreviate)

Email Address:

Are you a US citizen? Yes No

Country of Citizenship, List all:

2. Applicant Security Verification Information

Social Security Number or Passport # if International:	Date of Birth:	Gender :	Code Word: (ex: Mother's Maiden Name)
- - Pursuant to executive order 9397 and used for employment verification		Male Female	

Are you a Sworn Law Enforcement Officer (arresting powers)?

Yes No

If Yes, please enter your Agency's NCIC ORI:

Are you an Intelligence Analyst

Yes No

3. Employing Agency / Organization Information

Agency / Org Name:

Agency / Jurisdiction: Local State Federal Tribal Contractor Sponsored Applicant International User

Agency / Org Type: Law Enforcement Military Emergency Management Government/Other

Specify Government/Other:

Business Address:
(No P.O. Boxes)

Phone:

Alternate Phone:

4. Name and Description of Project, Justification of Access

Project or Law Enforcement related work description:

Manage TDEx Identities

Length of Access requested if membership is requested for a project or special event **From:** **To:**

5. Mark appropriate box for the administrator role requesting and what string (select only one role)

LEEP: NOE OE DR DEV SDL

	System Administrator		Database Administrator
	Security Administrator		Network Administrator
	Audit Administrator		System Management Operator (SMC)
	Quality Assurance Tester		Configuration Management
	Token Administrator		Backup Administrator
	Programmer		Tester

6. Mark appropriate box for the administrator role requesting and what string (select only one role)

Brokered System: NOE OE DR DEV SDL

	System Administrator		Database Administrator
	Security Administrator		Network Administrator
	Audit Administrator		System Management Operator (SMC)
	Quality Assurance Tester		Configuration Management
	Token Administrator		Backup Administrator
	Programmer		Tester

7. Mark appropriate box for the program office role requesting

	Service Provider Administrator (SP)	X	Identity Provider Administrator (IDP)

8. Signature

X

Requestor Signature MONTH / DAY / YEAR

X

Requestor Supervisor Signature MONTH / DAY / YEAR

X

Requested Brokered System Supervisor Signature MONTH / DAY / YEAR

X

Requested Brokered System ISSO Signature MONTH / DAY / YEAR

X

Trusted Broker Supervisor Signature MONTH / DAY / YEAR

X

Trusted Broker ISSO Signature MONTH / DAY / YEAR

X

Trusted Broker SSA Signature MONTH / DAY / YEAR

FD-889 Date _____ **FD-889A Date** _____ **GU Sec Trng Date** _____ **PU Sec. Trng. Date** _____ **Contractor Clearance Type** _____

Date Created_____ Date Suspended _____ Date Reactivated _____

NATIONAL DATA EXCHANGE (N-DEx) ACCOUNT ADMINISTRATION
TEXAS DEPARTMENT OF PUBLIC SAFETY
CRIME RECORDS SERVICE

The participating User Agency agrees to name an N-DEx Agency Administrator responsible for:

1. Acting as the single point of contact for N-DEx issues;
2. Ensuring compliance with this agreement, current and future versions of the CJIS Security Policy, Department policies and procedures regarding N-DEx, and all applicable state and federal laws;
3. Authorizing users from that User Agency to participate in the N-DEx system;
4. Creating user accounts through the user management tools provided by the system;
5. Suspending user access to the system when they leave the User Agency or otherwise become ineligible for access:
6. Ensuring that all users from that User Agency are trained and informed of policies and procedures that govern N-DEx;
7. Reporting security incidents to the Texas Department of Public Safety CJIS ISO, as required by the N-DEx User Agreement.
8. The participating User Agency must notify the N-DEx System State Administrator immediately whenever the incumbent N-DEx Agency Administrator is replaced by a new person.

The participating User Agency will ensure that only approved persons performing authorized functions have access to the N-DEx system.

FOR THE PARTICIPATING USER AGENCY:

User Agency Name	Date
User Agency Director (Signature)	User Agency Director (Print Name)
Agency Administrator assigned (Print Name)	Agency Administrator Phone Number

FD-889a Revised 5-15-2012 Previous Versions Obsolete	**FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form**

Purpose: This agreement outlines the acceptable and unacceptable uses of FBI privileged user access to FBI Information Technology (IT) and Information System (IS) resources. The additional access and behaviors required to perform privileged user activities imply the need for enhanced assurance of your competence to perform those activities and of your integrity in their performance. The role of privileged user constitutes a special category of user who can affect and effect the security of FBI IT and IS resources. For that reason, the privileged user agreement includes additional measures to ensure performance integrity and competence.

Scope: This agreement applies to anyone who is granted privileged user IT or IS access for any authorized purpose. Privileged users generally maintain the security attributes of users and of technologies for FBI systems and in that regard, privileged users have greater access to FBI IT and IS than does the normal general user.

Monitoring: I understand that as a privileged user, all my user activities are subject to monitoring by the FBI. Monitoring may entail an aggregated review of all of my system/network activities and data base entries and activities.

Statement of Responsibility: I understand that I am to use my privileged access to FBI systems for lawful, official use and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) and as further outlined in this document and other FBI policy directives. Even where granted access, I must only access the privileged user function in furtherance of authorized tasks or mission related-functions. To remain compliant with applicable statutes, orders, regulations, and directives, the FBI will update this form. It is my responsibility to maintain current knowledge of the FBI IT/IS Rules of Behavior for Privileged Users.

If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

Access: Privileged user access to FBI IT/IS, networks, and other agency systems operating in FBI spaces is granted for official and authorized purposes as set forth in the FBI Privileged User Program Policy and Title 5 CFR parts 2635 and 3801 (Federal Ethics Regulations) and as further outlined in this agreement.

Revocability: Privileged user access is a revocable privilege. Privileged user access may be revoked as a result of negative findings in official investigations of privileged user access. Failure to sign this form is grounds for revocation of privileged user access.

Rules of Behavior: As a Privileged User of FBI IT/IS, I will:

1. Abide by the provisions of the FBI IT/IS Rules of Behavior for General Users except those variations required to perform authorized privileged user activities.
2. Limit the performance of privileged user activities to my privileged user account(s).
3. Consent to monitoring and search of any IT/IS equipment that I use while in or bring into or remove from FBI owned, controlled, or leased facilities.
4. Complete FBI Privileged User Security Training.
5. Successfully complete any technical or administrative training required by the Head of my

Division that is related to competent and secure operation of IT and IS for which I have privileged user status.

6. Submit to additional investigation and monitoring of my privileged user activities as required to ensure integrity of my privileged user activities. This includes random monitoring of my activities and random polygraphs related to my privileged user activities.
7. Immediately report any anomalous incident, including errors and oversights related to my privileged user activities, to my Information System Security Officer (ISSO), Information System Security Manager (ISSM), or Chief Security Officer (CSO) according to the appropriate FBI Incident Response Plan.
8. Use my privileged user role and access to perform only authorized privileged user activities for the benefit of the FBI.
9. Protect my "root" or "super user" account including passwords and privileges at the highest level of data that it secures.
10. Change my privileged user account password every ninety (90) days or as required for security reasons.
11. Protect all output whether hard-copy, electronic, or optical according to FBI policy.
12. Perform virus and integrity scanning of any media that is to be used to transfer information into an FBI system.
13. Notify the ISSO when my privileged user access to the system is no longer needed (e.g. transfer, termination, leave of absence, or for any period of extended non-use). If I am an ISSO, then I will notify my CSO when my privileged user access is no longer needed.

Expressly Prohibited Behavior: Unless required as part of my official duties as a Privileged User of FBI IT/IS, I will not:

1. Share my privileged user access or privileges with any unauthorized person.
2. Use my privileged user access or privileges to "hack" any IT/IS (networked or non-networked).
3. Attempt to gain access to data for which I am not specifically authorized, to include e-mail and users files in their home directories.
4. Use my privileged user access for non-Government business.
5. Introduce any software or hardware that has not been approved through the FBI Change Management Process into FBI IT/IS, systems or networks.
6. Use any FBI communications, transmission, processing, or storage components for unauthorized purposes.
7. Disclose, without authorization, any personally identifying information (PII) that I access or learn as a result of my privileged user duties and activities.
8. Disclose, without authorization, any sensitive, classified, or compartmented FBI information that I access or learn as a result of my privileged user duties and activities.

Privacy Act Statement:

The information solicited on this form is collected pursuant to the Federal Information Security Management Act (FISMA) of 2002, the Computer Security Act of 1987, the general recordkeeping provision of the Administrative Procedures Act (5 U.S.C. 301) and Executive Order 13478, which permits the collection of social security numbers.

Pursuant to the Privacy Act of 1974 (5 U.S.C. § 552a), we are providing the following information on principal purposes and routine uses. The principal purpose of this form is to verify that individual signatories are aware of the rules of behavior that govern privileged access to FBI IT/IS that operate in FBI space.

The information on this form may be shared with DOJ components and other governmental agencies for the purpose of facilitating information sharing (i.e.-sending encrypted e-mails) and for other authorized purposes.

In addition, information may be disclosed to the following;

1. Appropriate federal, state, local, tribal, foreign or other public authorities conducting criminal, intelligence, or security background investigations.
2. Officials or employees of other federal agencies to assist in the performance of their duties when disclosure is compatible with the purposes for which the information was collected.
3. To contractors, grantees, experts, consultants, or others when necessary to accomplish an agency function.
4. Pursuant to applicable routine uses for the FBI's Central Records System (Justice/FBI-002), which is where the information solicited on this form will be maintained.

The provision of the information is voluntary, but without your acknowledgment of the privileged user rules of behavior for accessing FBI information and IT/IS's that operate in FBI space, you may not be permitted such access which may affect your ability to perform your official duties. Disclosure of the last four digits of your social security number is also voluntary, but will help to differentiate you from other individuals with the same or a similar name.

Acknowledgement

I acknowledge that I have read and understand the above listed Privileged User Rules of Behavior. I also state that I will adhere to these Privileged User Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of privileged user access to FBI IT/IS networks or facilities. I also understand that violation of these Privileged User Rules of Behavior will be reported to the appropriate authorities for further administrative, civil or criminal disciplinary action deemed appropriate.

Printed Name: _____ Date: _____

Employee Signature: _____ Last Four of SSN: xxx-xx- _____

FBI Division: _____ System Name: _____

FBI Personnel File Number (if known): _____

Note: If applicable, other Govt. Agency (Federal, state, or municipality):

Filing Instructions: Completion of the FBI's annual Privileged User Training satisfies the signatory and acknowledgement requirements for the purpose of storage and audit of this form. When a hardcopy is required, CSOs are responsible for filing this form IAW EC 319W-HQ-A1487698-SECD Serial 88.

Form Owner: Information Assurance Section, FBI SecD

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- US Code, Title 18, Section 798, Disclosure of Classified Information.
- Department of Justice (DOJ) Order 2640.2F, Information Technology Security.
- DOJ IT Security Standards.
- Corporate Policy Directive 71D, FBI Information Systems Use Policy.
- Corporate Policy Directive 74D, Security Monitoring of FBI Information Systems.
- Corporate Policy Directive 213D, FBI Information System Privileged User Program Policy.
- The Privacy Act of 1974 (as amended) 5 USC 552a.
- FD-291, FBI Employment Agreement.
- FD-857, Sensitive Information Nondisclosure Agreement.
- FD-868, Nondisclosure Agreement for Joint Task Force Members, Contractors, Detailees, Assignees, and Interns.
- FD-889, FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form.
- FD-1001 Consent for Warrantless Searches of Department of Justice Workplaces.
- SF-312, Classified Information Nondisclosure Agreement.
- Form 4414, Sensitive Compartmented Information Nondisclosure Agreement.

TEXAS DEPARTMENT OF PUBLIC SAFETY

CRIME RECORDS SERVICES

NATIONAL DATA EXCHANGE (N-DEx) USER/EQUIPMENT AGREEMENT

This document constitutes an agreement between the Texas Department of Public Safety (TXDPS), State Administrator of the National Data Exchange (N-DEx), P.O. Box 4143, Austin, Texas, 78765-4143 and a criminal justice or law enforcement agency, hereinafter referred to as the User Agency.

USER AGENCY _____

ADDRESS _____

The User Agency will ensure that only approved persons performing authorized criminal justice functions have access to N-DEx.

N-DEx information, including any analytical products derived there from, may not be used as a basis for action or disseminated outside User Agency for any purpose or in any other manner, unless the User Agency first obtains the express permission of the agency or agencies that contributed the information in question. Specifically included within this prohibition are any inclusion on N-DEx information in an official case file and any use of subpoenas. User Agency may not electronically retain N-DEx information without obtaining the N-DEx contributing agency's permission. When N-DEx information is summarized or otherwise documented, the User Agency shall indicate that the information was obtained from N-DEx.

Notwithstanding the requirement in the preceding paragraph that N-DEx information not be used as a basis for action or disseminated without first obtaining the permission of the contributing agency, in accordance with and to the extent permitted by applicable law, court process, or applicable guidelines, immediate dissemination on N-DEx information without such permission can be made if the User Agency determines that:

(a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to U.S. national security; and

(b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat, danger, or harm.

The User Agency shall immediately notify TXDPS and the N-DEx contributing agency if it disseminates any N-DEx information under this exception. Any requests for reports or information in N-DEx from anyone other than a party to this User Agreement will be directed to the N-DEx User Agency which contributed the data.

TXDPS RESPONSIBILITIES REGARDING N-DEx

TXDPS agrees to maintain, operate, and manage N-DEx communications and criminal justice information systems on a 24 hour, 7 day per week and 365 days a year basis. TXDPS further agrees to act as the State Administration Agency to facilitate the exchange of information between the User Agency and the following agencies: Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) National Data Exchange (N-DEx). TXDPS Driver's License Files (DL), Sex Offender Registration (SOR), Texas Department of Criminal Justice (TDCJ) probation/parole data and other data files may be implemented in future applications of information available to authorized users.

TXDPS reserves the right to restrict the type and scope of data to which the user may have access. TXDPS will provide system training to N-DEx users at no charge to the User Agency at a time and location to be designated by TXDPS. The obligation of TXDPS to incur training costs is conditional upon sufficient funds budgeted and available. No financial liability will be incurred by TXDPS by virtue of this agreement beyond monies available to it for the purpose of fulfilling this agreement.

TXDPS may provide or assist User Agency with the initial installation of adapter hardware, records management system (RMS) and/or jail management system (JMS) software enhancements or interface functionality(s). User Agency RMS and/or JMS software enhancements delivered as the result of custom developed N-DEx functionality are the property of the User Agency or User Agency RMS/JMS software vendor. User Agency is responsible for maintaining the capability to submit data to N-DEx following User Agency RMS/JMS enhancements or replacements.

TXDPS agrees to maintain its applicable N-DEx hardware, software and functionality including data adapter extraction and export methodology/technology plus future implementation(s) involving National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPDs). This determination may be made by TXDPS or its authorized designee.

N-DEx maintains an audit capability that will log the date, time, event type, and originating account of all user queries. N-DEx will maintain the audit logs for the life of the records accessed.

TXDPS reserves the right to immediately suspend service to the User Agency when applicable policies are violated. Service may be reinstated following such instances upon receipt of satisfactory assurances that such violations have been corrected. All costs for reconnection service are the responsibility of the User Agency. TXDPS shall have the authority to inspect and audit the equipment, records, and operations of the User Agency to determine compliance.

USER AGENCY RESPONSIBILITIES REGARDING N-DEx

The User Agency may only access and use N-DEx information for official criminal justice and national security purposes. N-DEx information cannot be accessed or used for any other purpose. User Agency agrees to allow TXDPS to share User Agency data contributed to N-DEx with other authorized criminal justice agencies.

The User Agency shall abide by all laws of the United States and the State of Texas, and shall abide by all present or hereinafter approved rules, policies and procedures of N-DEx and the CJIS Security Policy, concerning the collection, storage, processing, search, retrieval, dissemination and exchange of criminal justice information.

If the User Agency provides N-DEx derived criminal justice information to another criminal justice or law enforcement agency, which at that time is not operating through N-DEx pursuant to a N-DEx User Agreement, then it shall be the responsibility of the User Agency to verify that the non-user agency abides by the laws of the United States and the State of Texas and the operational policies of the applicable systems.

The User Agency agrees to appoint an N-DEx User Administrator responsible for:

a. Acting as the single point of contact for N-DEx issues;
b. Ensuring compliance with this agreement, current and future versions of policies and procedures regarding N-DEx, and all applicable state and federal laws;
c. Vetting, authorizing and managing users through the role based user management tools provided in N-DEx;
d. Terminating user access immediately upon user separation from the User Agency or otherwise become ineligible for access;
e. Ensuring that all users from that User Agency are trained and informed of policies and procedures;
f. Reporting security incidents to the TXDPS CJIS Information Officer (ISO), as is required by the User Agency's CJIS Security Addendum.

The User Agency must notify the N-DEx State Administrator immediately whenever the incumbent User Administrator is replaced.

User Agency certifies that all User Agency staff with access to N-DEx have undergone background checks consistent with Texas or federal requirements, so long as, at a minimum, those requirements included a criminal history and state and national fingerprint check.

The User Agency shall manage information system accounts, including establishing, activating, modifying, reviewing, and disabling accounts. The User Agency shall validate information system accounts at least annually and shall document the validation process.

Account management includes assignment of associated authorizations. The User Agency shall identify authorized users of the information system and specify access rights/privileges. The User Agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The User Agency shall be responsible for maintaining the User Agency RMS and/or JMS in good working order. The User Agency agrees to maintain its applicable hardware, RMS, JMS, and adapter interface functionality(s) to maintain complete and continual functionality with N-DEx. User Agency hardware (including workstations utilized to access), RMS, JMS and adapter interface shall be installed in a location where only authorized personnel have access.

The User Agency is responsible for providing its own internet connectivity and maintenance which meets CJIS Security Policy requirements.

Each N-DEx contributing User Agency retains sole ownership of, sole responsibility for, and exclusive control over the content of the information that it contributes to N-DEx, and each User Agency may, at will and at any time, update, correct, or delete the information that it contributes to N-DEx. Each N-DEx contributing User Agency has the sole responsibility to ensure that information that it contributes to N-DEx was not obtained and is not maintained in violation of any federal, state, or local law applicable to that User Agency.

In addition, each N-DEx contributing User Agency has the sole responsibility and accountability for ensuring compliance with all laws, regulations, policies, and procedures applicable to its entry and sharing of information into N-DEx. N-DEx User Agency will duly report to TXDPS and the contributing User Agency, in writing, any instance in which N-DEx information is used in an unauthorized manner. Such notice is to be provided in a timely manner within three days of when the party first learned of the unauthorized use.

Each N-DEx contributing User Agency has the duty, sole responsibility, and accountability to make reasonable efforts to ensure the accuracy, upon entry and continuing thereafter, of information that it contributes to N-DEx. Should TXDPS receive a challenge to, or reasonable question about, the accuracy of the information in N-DEx, TXDPS will notify the N-DEx User Agency.

Any User Agency data or process related to N-DEx that could affect and cause degradation of service to other N-DEx users must be authorized by TXDPS prior to implementation. TXDPS reserves the right to refuse such application on N-DEx should resources not be available, or in the best interest of the N-DEx users.

N-DEx USER AGREEMENT TERMINATION AND DURATION

This N-DEx User Agreement will enter into force on the day it is signed by the last party and it will remain in effect until terminated or modified by both parties. This N-DEx User Agreement may be terminated at any time upon the mutual written consent of the parties. In the event that both parties consent to terminate this N-DEx User Agreement, the parties will consult prior to the date of termination to ensure termination on the most economical and equitable terms.

Either party may terminate this N-DEx User Agreement upon 30 days written notice to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following will apply:

(a) The terminating party will continue participation, financial or otherwise, up to the effective date of termination.
(b) Each party will pay the costs it incurs as a result of termination.
(c) All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during a party's participation in this User Agreement shall survive any termination.

User Agency, to the extent authorized by law, agrees to indemnify and save harmless TXDPS, its Director and Employees from and against any and all claims, demands, actions and suits, including but not limited to any liability for damages by reason of or arising out of any false arrest or imprisonment or any cause of action whatsoever, arising out of or involving any negligence on the part of the User Agency or its employees in the exercise of enjoyment of this Agreement.

In WITNESS WHEREOF, the parties hereto caused this Agreement to be executed by the proper officers and officials.

USER AGENCY

By _____

* Must be individual who is authorized to contractually obligate the User Agency.

Title _____

Signature _____

Date _____