****

**User Agency Agreement**

**Between**

**U.S. Department of Justice**

**Criminal Justice Information Services Systems Agency**

**and**

**<Insert User Agency>**

**Background:** The United States Department of Justice (DOJ) Chief Information Officer (CIO) serves as the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Systems Agency (CSA) for DOJ, as well as other Federal and Tribal Agencies and entities. The DOJ CSA is responsible for establishing and administering an information sharing and information technology security program for its User Agencies, in order to protect DOJ information, systems, and services, as well as provide the appropriate controls to safeguard Criminal Justice Information (CJI) from creation through dissemination; whether at rest or in transit. The DOJ CSA facilitates this security through its Justice Criminal Information Services (JCIS; formerly known as DOJ Criminal Justice Information Network – CJIN), which provides access to the following national crime information systems for both criminal and non-criminal justice purposes:

* National Crime Information Center (NCIC) and Interstate Identification Index (III)
* Next Generation Identification (NGI)
* National Instant Criminal Background Check System (NICS)
* National Data Exchange (N-DEx)
* International Justice and Public Safety Network (Nlets)

A User Agency is the entity legally authorized by FBI CJIS to submit to or receive information from FBI CJIS systems, either as a Criminal Justice Agency or a Non-Criminal Justice Agency.

**Purpose:** This User Agency Agreement outlines the responsibilities of the DOJ CSA and the User Agency, with regard to access to the FBI CJIS systems.

# Responsibilities

The DOJ CSA and the User Agency agree to comply with the terms of this User Agency Agreement, and all applicable laws, regulations, and related requirements, to include those in the [FBI CJIS Security Policy (CSP)](https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center), all related FBI CJIS system-specific manuals, and the [Nlets User Policy Manual](http://wiki.nlets.org/index.php/Nlets_User_Policy). Additionally, the DOJ CSA and User Agency agree to comply with all directives and decisions of the criminal justice community’s Advisory Policy Board (APB), [National Crime Prevention and Privacy Compact Council](https://www.fbi.gov/services/cjis/compact-council), and all relevant DOJ specific policies, orders, and regulations. Dissemination controlled documents are available at www.CJIS.gov (LEEP).

## DOJ CSA Responsibilities

The DOJ CSA shall comply with the following responsibilities, as they pertain to the access of FBI CJIS systems through JCIS:

1. The DOJ CSA shall be responsible for User Agency and user discipline, and shall ensure compliance by User Agency with applicable statutes, regulations, and policies
2. The DOJ CSA will audit all User Agencies at least once every three years for the data and services to which the DOJ CSA authorizes access to verify User Agency and individual user compliance to applicable statutes, regulations, and policies
3. The DOJ CSA shall respond to Freedom of Information Act (FOIA) and Privacy Act requests in accordance with the 28 CFR 16.4(d)(2)(i) by referring all requests to the record-owning Agency if the Agency is subject to the FOIA.
4. The DOJ CSA shall monitor and automate logging of all successful and unsuccessful user logon attempts, file access, correlations, and transactions
5. The DOJ CSA shall institute quality assurance procedures for all User Agencies to ensure records are accurate, complete, up-to-date, valid, and disseminated properly and securely.
6. The DOJ CSA shall maintain overall control and visibility of security measures pertaining to JCIS or criminal justice information (CJI) obtained through JCIS and other DOJ CSA authorized systems such as physical security of communication equipment; personnel security; technical security; access control; data security; dissemination; logging; and security of criminal history records
7. The DOJ CSA shall provide User Agencies with Security Awareness and FBI CJIS system-specific training. This training is available via the online CJIN Training and Learning Center. The DOJ CSA may approve an Agency-developed training program, so long as it demonstrates compliance with the FBI CJIS Security Policy and DOJ CJIN Policy

## User Agency Responsibilities

1. Accountable Executive: The User Agency shall appoint an Executive to sign the User Agency Agreement with the DOJ CSA. The User Agency Executive is the accountable party for the User Agency, and enforces the FBI CJIS Security Policy and DOJ CJIN Policy over its user community. All applicable policies and training materials are available via the online CJIN Training and Learning Center. The User Agency Executive must appoint a Terminal Agency Coordinator (TAC) to carry out the responsibilities described in this User Agency Agreement and TAC Addendum. The User Agency Executive must notify the DOJ CSA within five business days if the individual serving as the TAC changes, as a new TAC Addendum must be signed by both the User Agency Executive and the new TAC
2. Audit: The User Agency shall comply with all FBI CJIS and DOJ CSA audit requirements (CSP 5.11.2)
3. Dissemination: The User Agency shall comply with all requirements regarding access, use, and dissemination of CJI and criminal history record information (CHRI), to include: (CSP 4.2; 28 CFR 20.33)

* Validating that the User Agency and user receiving the disseminated CJI and CHRI is an authorized recipient of such information
* Relying or acting upon CJI within the limitations specified by the record-owning Agency
* Ensuring all appropriate FBI CJIS-approved agreements are in place regarding access to and sharing of CJI

1. Hit Confirmation: The User Agency shall comply with all hit confirmation procedures (NCIC Operating Manual 1.3.1 & 3.5; DOJ CJIN Policy C)
2. Logging: The User Agency shall maintain an electronic log of all disseminated CHRI information that is provided to other authorized agencies (DOJ CJIN Policy B.4)
3. Quality Assurance: The User Agency shall comply with all quality assurance procedures, which include maintaining records that are accurate, complete, up-to-date, and valid (NCIC Operating Manual 3.1)
4. Screening (Pre-Employment): The User Agency shall demonstrate that it has policies and procedures in place that comply with the “Minimum Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI”, as set forth in the FBI CJIS Security Policy and DOJ CJIN Policy Manual. Additionally, the User Agency shall, where legal authority exists, ensure users meet minimum screening requirements prior to being granted access to CJI, and conduct record checks of all users with access to CJI every five years (CSP 5.12.1; DOJ CJIN Policy A. 1-3)
5. Security: The User Agency shall adhere to the security standards documented in the FBI CJIS Security Policy, which include personnel, physical and technical security, as well as user authorization and dissemination (CSP 5.5-5.10, 5.12-5.13)
6. Timeliness: The User Agency shall submit, modify, update, and remove data as soon as information is available, processed, and transmitted (NCIC Operating Manual 3.1)
7. Training: The User Agency shall ensure users receive training required for their level of access, including unescorted access to a physically secure location, before being granted access to CJI, and biennially thereafter. That training may be accomplished by using DOJ CSA provided materials via the online CJIN Training and Learning Center. Alternatively, the User Agency may utilize an Agency-developed training program, as long as it demonstrates the compliance with the FBI CJIS Security Policy and DOJ CJIN Policy. The User Agency shall maintain records of individual basic security awareness training and specific information training (CSP 5.2)
8. Use of the System: The User Agency shall ensure that all personnel use the DOJ CJIN systems only for the purposes for which they are authorized. Additionally, the User Agency shall be responsible for computer security incident reporting, as required by the FBI CJIS Security Policy (CSP 5.3.4; DOJ CJIN Policy B.3)
9. Validation: The User Agency shall have procedures in place for the annual validation of information system accounts, the biennial validation of Originating Agency Identifiers (ORIs), as well as required validation of submitted records to NCIC (CSP 5.5.1; NCIC Operating Manual 3.4)
10. Disclosure or Records: The User Agency acknowledges that information related to the use of any DOJ CJIN systems may be subject to FOIA and Privacy Act requests, and the User Agency shall respond appropriately (see 28 CFR 16.4)
11. Billing: The User Agency shall execute a billing Reimbursable Agreement (RA) with the DOJ CSA for the cost of the service(s), where required
12. Additional Fees: The User Agency, with the assistance of the DOJ CSA, shall execute a Memorandum of Agreement (MOA) with FBI CJIS to pay required User Fees associated with fingerprint-based and name-based Criminal History Record Information (CHRI) checks for non-criminal justice purposes

# General Provisions

## Termination

1. This agreement may be amended or terminated by the mutual written consent of the User Agency Executive and DOJ CJIS Systems Officer (CSO)
2. Either Agency may terminate this User Agency Agreement with thirty days written notice to the other party. In the event of such termination, the following rules apply:
   1. The parties will continue participation, financial or otherwise, through the effective date of termination
   2. Each party will pay the costs it incurs as a result of termination
   3. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement

# JCIS Access

An FBI-issued DOJ CSA ORI shall be used in each transaction on FBI CJIS systems to identify the sending Agency and to ensure the proper level of access for each transaction. The level of system access is based on the legal authority under which the ORI is issued, and the authorization of the DOJ CSA.

## The User Agency shall select what access to NCIC it requires:

Full NCIC Access: This allows the User Agency to query and enter records. User Agencies must comply with security standards, record accuracy, timeliness, completeness, and validation specifications, hit confirmation policy, and training requirements contained in the NCIC Operating Manual

Limited NCIC Access: This allows the User Agency to query records only. User Agencies must comply with security standards, hit confirmation policy, and training requirements contained in the NCIC Operating Manual

No NCIC Access

## The User Agency shall select what access to NICS it requires:

NICS Indices Entry Access: This allows the User Agency to enter information on persons prohibited from receiving firearms, when it cannot be entered as part of an arrest disposition or does not meet the NCIC file entry requirements. The prohibiting information includes substance abuse information and mental health adjudications. The User Agency must comply with data integrity and safeguarding requirements, as well as system access requirements contained in Title 28 CFR 25 Subpart A

NICS Query Access: This allows the User Agency to perform queries of NICS for the purpose of providing information in connection with the issuance of a firearm-related permit or license, and disposing of firearms in the possession of a Criminal Justice Agency. The User Agency must comply with data integrity and safeguarding requirements, as well as system access requirements contained in Title 28 CFR 25 Subpart A

No Access to NICS or NICS Indices

## The Agency shall select what access to N-DEx it requires:

N-DEx Access: This allows the User Agency to query, link, analyze, and share local, state, Tribal, and Federal records that are not contained in NCIC, III, and NGI, such as incident/case reports, incarceration data, and parole/probation data. The User Agency must comply with training requirements, as well as record accuracy, timeliness, and completeness standards contained in the N-DEx Policy and Operating Manual

No N-DEx Access

## The User Agency shall select what access to NGI it requires:

Criminal Justice Access: This allows the User Agency to query and submit biographic and biometric data for offender identity verification, criminal history record management (i.e. Identity History Summary, also known as the Rap Sheet), and sex offender registration. The User Agency acknowledges that submitted information may be made available to other national crime information systems, such as N-DEx. Additionally, the User Agency must comply with the arrest disposition submission standards required by FBI CJIS and Title 28 CFR 20.37, which states that it is the responsibility of each Criminal Justice Agency to ensure that information on individuals be kept complete, accurate, and current, so that all such records shall contain dispositions for all arrest data included therein. Criminal justice agencies should submit dispositions within 120 days after the disposition has occurred

Non-Criminal Justice Access: This allows the User Agency to submit fingerprints for expedited national Identity History Summary checks for non-criminal justice purposes. The User Agency must comply with the FBI CJIS Security Policy Criminal History Record Information (CHRI) controls and Personally Identifiable Information (PII) policy

No NGI Access

# User Agency Agreement Signatory Page

Each party hereby acknowledges the requirements set out in this User Agency Agreement. The User Agency further acknowledges that a failure to comply with these requirements may subject the User Agency to DOJ CSA sanctions that range from suspension of access to termination of services.

The User Agency Agreement is a formal expression of the purpose and intent of both parties and is effective when signed by both parties. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. Accordingly, this agreement will remain in effect regardless of DOJ CSO and/or User Agency Executive personnel changes, until it is amended in writing or rescinded.

X

User Agency Executive Signature Date

User Agency Executive Printed Name Agency and Title

X

DOJ CJIS Systems Officer Date

Law Enforcement Services & Information Sharing

DOJ Office of the Chief Information Officer