Agenda Item No: CA-d
Meeting Date: July 25, 2022

Subject: Consent Agenda Item

CA-d Approval of Resolution 22-55, approving a User Agreement for CBI-CJIS Systems Access for Non-Criminal Justice Agency.

The City Clerk's Office uses the Colorado Bureau of Investigation-Criminal Justice Information Services System to access fingerprint results for background checks for Liquor License Applicants.

The Colorado Bureau of Investigation requires each agency to approve the User Agreement in order to maintain access to such records and outlines the responsibilities of each agency.

RESOLUTION NO. 22-55

A RESOLUTION APPROVING A USER AGREEMENT FOR CBI-CJIS SYSTEMS ACCESS FOR NON-CRIMINAL JUSTICE AGENCY

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF DACONO, COLORADO:

Section 1. The User Agreement for CBI-CJIS Systems Access for Non-Criminal Justice Agency is hereby approved in essentially the same form as the copy of such Agreement accompanying this resolution.

Section 2. The Mayor is hereby authorized to execute the Agreement on behalf of the City, and is further authorized to negotiate and approve on behalf of the City such revisions to the Agreement as the Mayor determines are necessary or desirable for the protection of the City, so long as the essential terms and conditions of the proposal are not altered.

INTRODUCED, READ, and ADOPTED this 25th day of July, 2022.

CITY OF DACONO, COLORADO

_____
Adam Morehead, Mayor

ATTEST:

_____
Valerie Taylor, City Clerk

COLORADO
Bureau of Investigation
Department of Public Safety
690 Kipling Street, Suite 3000
Denver, CO 80215

User Agreement for CBI-CJIS Systems Access for Non-Criminal Justice Agency

1. Purpose

The purpose of this User Agreement is to outline the responsibilities the Colorado Bureau of Investigation (CBI) maintains as the operating agency of the Colorado Crime Information Center (CCIC) Computerized Criminal History database (CCH) and the Secure Document Delivery System (SDDS) Criminal Justice Information Systems. These systems are collectively referred to as the CBI-CJIS Systems. The CBI agrees to furnish to the Non-Criminal Justice Agency (NCJA), hereafter called the Agency, criminal justice information through the CBI-CJIS Systems subject to the provisions contained herein. The scope of this User Agreement also extends to the contribution of fingerprint submissions to the CBI.

1.1. Policy

The CBI is the CJIS Systems Agency (CSA) for the State of Colorado. Pursuant to the User Agreement between the CBI and the Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Division, the CBI adopts the FBI-CJIS policies—including but not limited to the CJIS Security Policy—as the standard for all Colorado CJIS systems. Additionally, all operating policies, manuals, and procedures specific to CCIC and SDDS are incorporated by reference. It is the CBI policy that all data contained within the CCIC and SDDS computer systems are considered Criminal Justice Information (CJI) and may only be accessed and/or disseminated as specifically prescribed and authorized by Colorado law.

The CBI maintains and operates the CCIC computer system under shared management pursuant to this User Agreement. CCIC houses CCH and provides information from the National Crime Information Center (NCIC) and the Interstate Identification Index (III). A Terminal Agency Coordinator (TAC) is designated for each Agency, and is responsible for that Agency's use, security, and personnel who operate CJIS systems. All parties will operate in accordance with Colorado and Federal law; this User Agreement shall be governed, construed, and enforced in accordance with the laws of the State of Colorado. This User Agreement shall not be amended as any amendment would require a new version of this agreement produced by the CBI and signed by all parties.

1.2. Governing Standards

The Agency shall access, retain, submit, and destroy all CJI following the requirements within the laws, policies, and manuals listed below and incorporated into this agreement by reference herein.

- Title 28, Code of Federal Regulations, Part 20
- CJIS Security Policy
- The National Crime Prevention and Privacy Compact, Title 34 of the United States Code, Chapter 403, Subchapter II

- Security and Management Outsourcing Standard for Non-Channelers (Outsourcing Standard)
- Colorado Open Records Act (CORA)/Colorado Criminal Justice Records Act (CCJRA)
- Any and all Colorado Laws specifically pertaining to the collection and use of fingerprints for and by the Agency
- CBI Misuse Policy
- Secure Document Delivery System Manual

1.3. Definitions

Agency: A non-criminal justice agency subject to the included standards throughout this agreement
Agency Head: The Chief Executive, or the member of the Agency appointed as the authority responsible for the operations of the Agency
Agency Personnel: Individuals working for the Agency in any capacity, including employees, volunteers, vendor support staff, and contract staff
CBI: Colorado Bureau of Investigation
CCIC: Colorado Crime Information Center
CCH: Computerized Criminal History Database
CHRI: Criminal History Record Information, a subset of CJI
CJA: Criminal Justice Agency
CJI: Criminal Justice Information
CJIS: Federal Bureau of Investigation's Criminal Justice Information Services
CJIS System: Any computer system containing information derived from CCIC CCH, or the FBI CCH
Compact: The National Crime Prevention and Privacy Compact Act of 1998
Compact Officer: The chief administrator of the Colorado criminal history record repository
CORA: Colorado Open Records Act
CSA: CJIS Systems Agency
CSA ISO: CJIS Systems Agency Information Security Officer; the appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies
CSO: CJIS Systems Officer
FBI: Federal Bureau of Investigation
III: Interstate Identification Index
Individual User: An employee of an NCJA with access to CJIS information
LASO: Local Agency Security Officer
Live scan: A device or machine used to obtain and/or transmit electronic fingerprint captures
MBIS: Morpho Biometric Identification System; the statewide fingerprint repository owned and maintained by the CBI
NCIC: National Crime Information Center
Operator: An individual user of CJIS data with direct access to CJIS systems
ORI: Originating Agency Identifier
Outsourcing: Obtaining services to store, access, or support CHRI lawfully obtained by the Agency to any governmental or non-governmental entity
Outsourcing Standard: The standard for outsourcing agreements as mandated in the National Crime Prevention and Privacy Compact Council document, ***"***Security and Management Control Outsourcing Standard for Non-Channelers"
PII: Personally Identifying Information
SDDS: Secure Document Delivery System
SDDS Administrator: The primary point of contact at the Agency for access to the Secure Document Delivery System
Terminal Agency: An Agency that accesses data derived from the CCIC and NCIC computer systems

TAC: Terminal Agency Coordinator
UCR: Uniform Crime Reporting

2. CBI CJIS Systems Agency (CSA) Responsibility

The CBI serves as the Colorado CJIS Systems Agency (CSA). As such, the CBI will provide access to CCIC, NCIC, and SDDS as lawfully authorized. Furthermore, the CBI will provide operational support including:

1. Legal and legislative review of matters pertaining to CJIS systems;
2. Operational, technical, and investigative assistance to personnel using CJIS systems;
3. Provision of training and materials to the TAC to assist with their respective Agency training responsibilities;
4. Assistance in investigating and rectifying incomplete, incorrect, or misidentified criminal records or other files;
5. The CBI is the custodian of CCIC records. Public requests, subpoenas, and other requests for any CCIC information shall be referred to the CBI for review and response.
6. Approval of outsourcing to private contractors and external governmental agencies (such as consolidated information technology departments).

Costs associated with provision of these services will be paid by the CBI through budgeted funds to include fingerprint fees.

3. Agency Responsibility

The Agency is responsible for providing adequate security and support for CJIS systems access at the Agency. The Agency is ultimately responsible for ensuring all responsibilities listed in sections 5, 6, and 7 of this document are satisfied.

The CBI will leverage agency network services, whether dedicated line or internet service, and assist the Agency in configuring adequate security using agency-provided software and hardware. Costs associated with purchasing, maintaining, and securing agency network equipment will be paid by the Agency.

The Agency may assign any of the duties listed above to a single person, or to separate individuals. Although responsibilities are delegated to one or more individuals, the Agency is ultimately accountable for ensuring all responsibilities are met.

When a new TAC, LASO, billing contact, and/or Agency Head are designated, the Agency Head will notify the CBI Compact Officer in writing within ten days of the appointment.

3.1. Key Roles

Each Agency shall appoint personnel to the following roles and allow sufficient resources to perform all listed duties. The Agency may assign key roles to a single person, or to separate individuals. Once the CBI has approved outsourcing by the Agency, roles may be assigned to outsourced personnel, including employees of contractors or external Information Technology departments or divisions. Although responsibilities are delegated to these roles, the Agency is ultimately accountable for ensuring all responsibilities are met.

Terminal Agency Coordinator (TAC)

The TAC unifies the Agency responsibility for individual user actions and serves as a CBI point of contact

700 Kipling Street Suite 1000, Lakewood, CO 80215 cdpsweb.state.co.us
Jared Polis, Governor | Stan Hilkey, Executive Director

for quality control, dissemination of manuals and other publications, training, audits, and any other matters concerning the use and misuse of CJIS systems. The TAC provides oversight for all CJIS systems and programs within the Agency and oversees the Agency's training and compliance with CJIS policies.

Local Agency Security Officer

The LASO is the primary information security contact between the Agency and the CSA under which this Agency interfaces with the FBI-CJIS Division. The LASO actively represents their Agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists the TAC with information security audits of hardware and procedures, and keeps the CSA informed as to any information security needs and problems.

SDDS Administrator

The administrator will perform all necessary duties related to the approval of SDDS user access and the security of the information therein.

Billing Contact

Each Agency that submits non-criminal applicant fingerprints for licensing--or employment external to the criminal justice agency--shall designate a primary point of contact for billing.

3.1.1. TAC Responsibility

The TAC shall:

1. Maintain the most current versions of the CJIS Security Policy, Outsourcing Standard, and SDDS Policies, making them available to the appropriate personnel. The Agency Head and TAC are also responsible for enforcing the policies contained in these documents;
2. Ensure all staff are provided adequate training for their responsibilities, duties, and degree of CJIS systems access or use;
3. Appropriately manage operator access to CJIS systems to include determining appropriate access and terminating access immediately upon separation of the employee;
4. If the separated employee had to undergo a fingerprint-based background check, alert the CBI that the separated employee no longer works for the Agency so that the CBI can deflag the employee in CCIC for subsequent arrest notification purposes;
5. Disseminate essential system-related bulletins as needed to relevant Agency personnel;
6. Report any allegation or findings of misuse of CJIS information by Agency personnel to the CBI;
7. Provide information regarding CJIS systems use at the local Agency to the CBI as the state CSA. This responsibility includes, but is not limited to:
    a. Detecting, reporting, and cooperatively investigating any unauthorized access ("misuse") of CJIS systems with the CBI immediately;
    b. Providing information to the CBI for the purpose of the background investigation regarding each individual user;
    c. Providing and maintaining copies of agreements with non-criminal justice agencies and businesses with access to local agency CJI.
8. The TAC assumes all responsibilities of the LASO if a separate individual has not been appointed LASO duties for the Agency.

700 Kipling Street Suite 1000, Lakewood, CO 80215 cdpsweb.state.co.us
Jared Polis, Governor | Stan Hilkey, Executive Director

9. The Agency Head and/or TAC may appoint one or more alternate TACs to assist with one or more of these duties.
10. The TAC shall be responsible for ensuring adequate CCIC training for operators within the Agency to include:
    a. Providing necessary training for newly hired operators;
    b. Ensuring completion of security awareness training once every two years;
    c. Maintaining documentation of any and all CJIS and fingerprinting training attended.

3.1.2. Local Agency Security Officer (LASO) Responsibility

The LASO shall:

1. Maintain the most current versions of the CJIS Security Policy, Outsourcing Standard, and Interface Control Document, making them available to the appropriate personnel. The Agency Head and LASO are also responsible for enforcing the policies contained in these documents;
2. Identify who is using the CSA approved hardware, software, and firmware, and ensure no unauthorized individuals have access to the same;
3. Identify and document how any local agency interface is connected to the state system;
4. Ensure that personnel security screening procedures are being followed as stated in this policy;
5. Ensure the approved and appropriate security measures are in place and operational;
6. Support policy compliance and ensure the CJIS Systems Agency Information Security Officer (CSA LASO) is promptly informed of all security incidents where CJI may be affected.

3.1.3. SDDS Administrator Responsibility

The SDDS Administrator shall:

1. Ensure SDDS results are reviewed at least weekly and information to be maintained from SDDS is downloaded and stored in a secure area or system as defined in the CJIS Security Policy;
2. Ensure each individual user of the SDDS is issued unique credentials;
3. Ensure access to the SDDS is terminated when a user no longer requires access, or separates employment from the Agency.

3.1.4. Billing Contact Responsibility (where applicable)

Where the Agency pays the CBI directly for services, a designated contact will be required to ensure the CBI and the Agency can communicate regarding any billing related matters.

3.2. Outsourcing

Many agencies contract with external private or public entities, such as County IT departments, or businesses providing data services, to perform services related to information technology and operational support.

Prior to outsourcing CJIS Services, the Agency shall request and receive written permission from the CBI Compact Officer as mandated in the Outsourcing Standard, section 2.

3.3. Audit Responsibilities

The CBI will conduct an audit for each Agency at least once every three years. Additionally, the FBI audit staff will conduct audits at least once every three years. This audit shall include a sample of non-criminal justice agencies in Colorado who are authorized recipients of CJI. The objective of this compliance audit is

to verify adherence to CBI and FBI policies and regulations.

The Agency is responsible for performing internal audits of outsourced services as mandated in the Outsourcing Standard.

The TAC is the primary point of contact for audit information. Audit information requested for CBI or FBI auditing purposes is to be provided in a complete and timely manner. The LASO shall provide technology security audit information through the TAC.

The CBI will cover costs to audit any Colorado non-criminal justice agency and/or data center in Colorado used by these agencies. It is the responsibility of the contracting agency to pay travel and lodging costs for audits of these facilities (to include data centers where CJI is stored) outside of Colorado.

3.4. Personnel Security and Training

Fingerprint-based background checks shall be required by all agency personnel where mandated by Colorado law. Pursuant to the Outsourcing Standard and the CJIS Security Policy, this will also extend to contractor personnel performing outsourced services. Contractor personnel shall undergo fingerprint-based background checks prior to servicing agencies where agency personnel are required to undergo fingerprint-based background checks. When fingerprinting is required, it is required for all personnel and contractors with direct, indirect, or incidental access to CJI (including but not limited to janitorial, maintenance, IT staff, HR staff, and those with direct read/write system access). Access to CJI must be denied to any personnel or contractor whose background check includes a felony conviction.

Regardless of whether a background check is performed, all personnel are also required to successfully complete CJIS-specific Security Awareness Training six months after initial assignment and biennially thereafter.

3.5. Operator Access

Operators with direct access shall be trained and successfully obtain user certification within six months of assignment and shall recertify biennially thereafter (this certification includes Security Awareness Training). The Agency is responsible for actions of Agency personnel using CJIS systems and data derived from CJIS systems. All systems submitting or receiving CJI or PII shall uniquely identify each user. Any violation of the policies incorporated in this agreement shall be prohibited by the Agency, including but not limited to:

- Sharing of user credentials for access to CJIS Systems;
- CJIS access from publicly accessible computers shall be considered a violation of this agreement;
- CJIS access shall be prohibited for individuals using personally owned information systems. The CBI may provide written approval for agencies that provide a detailed policy for use of personal information systems which complies with the standards of the CJIS Security Policy.

Each Agency shall set standards of discipline for violation of CJIS policy and document such standards. This can include incorporating the management of CJIS policy violations into agency policies for other disciplinary actions.

3.6. Purpose Code X Queries

When an emergency placement is necessary and a prospective relative or other available person is identified, and child(ren)/youth are placed into temporary custody by law enforcement and/or the court with a county department of human or social services, the county department shall conduct an initial name-based state and federal criminal history record check. To complete the name-based record check, the county department can contact their local law enforcement to conduct the check and receive the results verbally or the county department can conduct the check themselves if they have access to CCIC/NCIC. Pursuant to Colorado Revised Statute 19-3-406, fingerprints submitted for emergency placement of a child shall be submitted within five days of placement of the child, or within 15 days in exigent circumstances per FBI mandate.

If the child is not placed or fingerprints are not going to be submitted after the name-based criminal history record check is conducted, the county department shall provide the CBI, upon request, with the reason fingerprints will not be submitted.

3.7. Electronic Fingerprint Submission

Applicants should be referred to the Colorado Applicant Background Services (CABS) program site for submission of fingerprint-based background checks.

Agencies electing to maintain their own live scan fingerprint equipment shall meet the following standards:

1. Each Agency owning, leasing, and/or operating a live scan machine for electronic submission of fingerprints shall incorporate the technical standards of the CBI live scan Interface Control Document;
2. Live scan equipment shall be manufactured and/or supported by an FBI and CBI approved vendor;
3. Machines shall meet image quality specifications designated by the CBI and FBI, and be maintained regularly to sustain that image quality;
4. All civil live scan submissions shall meet the quality standards and specifications mandated for the Colorado Applicant Background Services and maintain an acceptance rate of 98%;
5. All systems submitting or receiving CJI or PII shall uniquely identify each user;
6. Adequate hardware and software support shall be maintained to ensure systems remain patched, functional, and secure.

3.8. Submitting Duplicate Transactions

Each Agency that submits fingerprints, either electronically or by mail, is responsible for all charges and fees incurred by such submittal. If a fingerprint submission is submitted multiple times and duplicate charges incur, it is the Agency's responsibility to pay all associated charges and fees resulting from the duplicate transactions.

Duplicate submissions of identical fingerprint submissions for different or multiple state statutes are not acceptable. A separate set of fingerprints needs to be taken and submitted for each state statute that mandates a fingerprint-based background check.

If a fingerprint submission is rejected for low quality and a resubmission is necessary, a new set of

fingerprints will need to be taken and submitted. Fingerprints identified as being sent previously will not be accepted. Such submission is a violation of policy per the Criminal Justice Information Services Division (CJIS) Information Letter dated June 2021, page 2, and "The second submission must have been a new collection of fingerprints. This procedure will be enforced through policy and audit."

4. Sanctions for Violations

The CBI may sanction the Agency for failure to meet the standards of the policies referenced in this document.

If a CBI audit identifies policy violations, the CBI will report the findings to the Agency in violation and request a mitigation plan. Failure to mitigate audit findings will result in sanctions as directed by the CBI Director, CJIS Systems Officer, and Compact Officer.

The CBI may impose sanctions on individual operators if an operator is found to have used CBI-CJIS systems in a manner that is against FBI and/or CBI policy, whether for unauthorized access, improper dissemination, unfounded query, or other use of the system that is not pursuant to state laws. These sanctions may include corrective training, temporary suspension, or permanent revocation of access.

5. Certification

Once signed, return **THE FOLLOWING PAGE ONLY** to:

CBI Biometric Identification and Records Unit
690 Kipling Street, Suite 3000
Denver, Colorado 80215.

Alternatively, this form may be emailed to CDPS_CBI_Ident_TAQC@state.co.us.

End of Agreement

700 Kipling Street Suite 1000, Lakewood, CO 80215 cdpsweb.state.co.us
Jared Polis, Governor | Stan Hilkey, Executive Director

NON-CRIMINAL JUSTICE AGENCY USER AGREEMENT FOR CJIS SYSTEMS ACCESS: ACKNOWLEDGMENT

As an Agency accessing and contributing to CJIS systems within the state of Colorado, we hereby acknowledge the responsibilities as set out in this document as well as those documents incorporated by reference. The Agency also agrees to comply with all state and federal statutes and regulations as may apply, and to use the information received over CJIS systems only for purposes specifically authorized by Colorado law.

We acknowledge these responsibilities have been developed and approved by the CBI and/or the FBI in order to ensure the security, reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of CJIS systems.

We acknowledge a failure to comply with these responsibilities will subject the CBI and this Agency to various sanctions as recommended by the Directors of the CBI and/or the FBI.

The CBI reserves the right to suspend service to the Agency, connected system, or an individual user when the security or dissemination requirements are violated to preserve the integrity of the system or any data obtained from the system. The CBI may reinstate service upon receipt of satisfactory assurance that violation(s) have been corrected. Either the CBI or the Agency may discontinue service upon thirty days' advance written notice. This agreement shall remain valid until terminated by either CBI or the Agency.

IN WITNESS WHEREOF, the parties hereto caused this agreement to be executed by the proper officers and officials. This agreement will become effective upon the date signed.

Agency Name: _____

Account Number(s) starts with CONCJ: _____

(existing accounts only – new accounts will be filled in by CBI)

Note: All 3 signatures are required - See 3.1 for TAC & LASO responsibilities

Signature of Agency Head	**Title and Printed Name**	**Date**
Signature of Terminal Agency Coordinator (TAC)	**Title and Printed Name**	**Date**
Signature of Local Agency Security Officer (LASO)	**Title and Printed Name**	**Date**

CBI Use Only Below

Signature of CBI Director/Designee	**Title and Printed Name**	**Date**

700 Kipling Street Suite 1000, Lakewood, CO 80215 cdpsweb.state.co.us
Jared Polis, Governor | Stan Hilkey, Executive Director