



CJIS VENDOR AGREEMENT

CJIS COMPUTER SYSTEMS

COLORADO BUREAU OF INVESTIGATION

1. Purpose:

The intent of this agreement and the policies and procedures herein is to facilitate compliance in Colorado with FBI-CJIS policy. The Colorado Bureau of Investigation (CBI), as the CJIS Systems Agency (CSA) for the state of Colorado, agrees to provide supporting services to private and public entities contracted by any Colorado Contracting Government Agency (CGA). To ensure vendor personnel undergo a fingerprint-based background check and to ensure audits of CJIS systems are accurate and consistent, the CBI will provide the policies and systems to allow background check results for a vendor employee to be accessible to CGA's and to allow audit findings from Shared CJIS Systems to be accessible to CGA's.

2. Policy:

As CSA, the CBI maintains and operates the CCIC computer system under shared management pursuant to the CCIC and NCIC User Agreements. As part of these agreements, the CBI establishes and enforces policies ensuring compliance with the FBI CJIS Security Policy. Section 5 of the CJIS Security Policy mandates background checks and audits are performed within each state under the authority of the CSA. The services defined in this document are intended to improve statewide compliance with the CJIS security policy.

Definitions:

Access (to Criminal Justice Information) — The physical or logical (electronic) ability, right or privilege to view, modify or make use of CJ.

Board of Executive Directors (BED) — The Executive Board within the CCIC Advisory Board consisting of Chiefs, Sheriffs, and other selected CJA Chief Executives.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJ from various systems managed by the FBI CJIS Division.

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 vendor.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce

the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJ refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJ: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJ or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJ to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Direct Access — Defined in the CJIS security policy as: (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency. (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Indirect Access – Defined in the CJIS security policy as: Having the authority to access systems containing CJ without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Personally Identifiable Information (PII) – PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Shared CJIS System – An outsourced, individual computer system which contains CJ, and which provides access/service to multiple CGA's. Examples include cloud storage systems and regionalized Computer-Aided Dispatch (CAD) systems.

Vendor – A private contractor providing services to a criminal justice agency which require, or in performance of work provide, access to CJ.

Vendor Services Coordinator (VSC) — A staff member of the Contracting Government Agency who manages the agreement between the vendor and agency.

3. CBI CJIS Systems Agency (CSA) Responsibility:

The CBI serves as the Colorado CJIS Systems Agency (CSA). As such, the CBI will provide connectivity to CCIC, NCIC and Nlets and provide operational support. Additionally, CJIS Vendors will be provided with services to reduce the cost and burden of CJIS compliance to the vendor and CGA's alike. These

consolidated services will allow CJIS Vendors to undergo these processes once for the state, instead of once for each CGA within the state and include:

3.1. Fingerprint-Based Background Check

The CBI shall ensure fingerprints submitted for background checks mandated by the CJIS Security Policy, section 5.12.1.2 are processed and results are available to CGA's. This will ensure each vendor employee may submit one set of fingerprints to one CGA and support all of the vendor's CGA's. Fingerprints must be submitted through a Colorado CGA.

3.1.1. CGA Background Checks

The CGA may elect to perform their own background check on a vendor employee, even where the vendor has completed a fingerprint based background check elsewhere within Colorado.

3.2. Audit

Every three years, the CBI will conduct audits of each criminal justice agency. As part of those audits, the CBI reviews services and systems provided by vendors to CGA's. Many CGA's use shared CJIS systems in order to improve information sharing or to reduce support costs. The CBI reserves the authority to determine whether shared CJIS systems are audited separately for each CGA, or once for all CGA consumers of the service. Consolidated findings of policy violations by the vendor shall be reflected in the audits of the CJIS Vendor's supported CGA's. Additionally, the FBI audit staff will conduct audits at least once every three years. This audit shall include a sample of state and local criminal justice agencies.

3.2.1. External Audits – In Lieu of CBI Audit

The CBI may accept audits provided by external entities in lieu of performing a separate audit.

3.2.2. Sanctions for Violations

The CBI may sanction CGA's and vendors for failure to meet the standards of the policies referenced in this document. Sanctioned agencies shall work collaboratively with their respective vendors to develop and report mitigation plans and timelines to achieve compliance. The CBI will implement sanctions under advisement of the BED and reserves the right to revoke vendor and CGA access for failure to accomplish CJIS compliance.

3.2.3. Confidentiality

The CBI will share vendor audit findings with CGA's. Requests for detailed information which may comprise trade secrets, security vulnerabilities, or other types of information determined to be sensitive by the CBI discovered or revealed through CJIS security processes will not be shared with the CGA. The CGA will be referred directly to the CJIS Vendor for access to any information not provided by the CBI.

4. Vendor Responsibility:

The CJIS Vendor shall comply with all applicable standards of the CJIS security policy. These standards may apply differently to different CJIS Vendors depending on the services provided. The Vendor shall

work proactively with their CGA(s) to ensure responsibility of contract parties related to CJIS compliance are appropriately assigned and maintained.

Each Vendor shall appoint a Contracted Services Coordinator (CSC). The CSC administers CJIS systems programs and oversees compliance with CJIS systems, CCIC and Nlets policies. Individual duties of the CSC may be delegated to a designee where the designee has specialized authority or knowledge.

When a new CSC is designated, the vendor representative will notify the CBI Crime Information Management Unit in writing of that appointment within ten days of the appointment.

4.1. Incorporated Standards

Vendors with direct access or indirect access to CJ shall handle all CJ following the requirements of the laws, and policies listed below and incorporated into this agreement:

- CJIS Security Policy
- Title 28, Code of Federal Regulations, Part 20 (relevant standards)

Vendors supporting systems which provide direct access to CJ shall also follow the regulations listed in the laws, polices and manuals incorporated into this agreement:

- NCIC Operating Manual
- CCIC Training Manual
- National Fingerprint File Operating Manual
- Title 28, Code of Federal Regulations, Part 23

4.2. Fingerprinting

The Vendor shall ensure fingerprints are submitted for background checks of each Vendor employee working with CJ. The Vendor is responsible for all fees associated with fingerprint processing and CJIS rap-back services where available.

4.3. Audit Responsibilities

Audit information requested by CBI or FBI auditing purposes is to be provided in a complete and timely manner.

4.4. CJIS Data Access:

Vendor staff members shall be trained in information security awareness pursuant to the CJIS security policy within six months of assignment and shall recertify biennially thereafter.

4.5. Other agreements:

Each CJIS Vendor may have one or more contracts with CGAs. Pursuant to the CJIS Security Policy, the CJIS security addendum shall be incorporated in all such contracts. Due to the diverse nature of CJIS Vendor businesses, the CBI may elect to sign a secondary agreement to supplement this agreement. Any secondary agreement shall be available for CGA and FBI review.

5. Vendor Services Coordinator (VSC) Responsibility:

The VSC unifies agency responsibility for individual user discipline and serves as the primary CBI point of contact for handling all matters concerning the use and misuse of CJIS systems. The VSC is the primary point of contact during CBI audits.

5.1. Contracting Government Agency

This agreement remains separate of all contracts between the CJIS Vendor and CGAs. Issues which may arise between the vendor and the CGA shall be resolved between the contract parties.

Pursuant to their CCIC User agreements, CGAs are responsible to determine how they can use the vendor's services in a manner compliant with the CJIS Policy. CGAs' compliance with the CJIS Policy will be dependent, in part, upon CGAs individual use of contracted services.

End of Agreement



CBI CJIS SYSTEMS VENDOR AGREEMENT ACKNOWLEDGMENT

As a CJIS Vendor supporting 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 Vendor also agrees to comply with all state and federal statutes and regulations as may apply, and to use the information received over CJIS systems for criminal justice purposes only.

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, CGA and this Vendor to various sanctions as recommended by the NCIC Advisory Policy Board, the BED, and/or the respective Directors of the CBI and/or the FBI.

To preserve the integrity of CCIC, the CBI reserves the right to suspend service to the CGA, Vendor, connected system, or an individual system user when the security or dissemination requirements are violated. The CBI may reinstate service upon receipt of satisfactory assurance that violation(s) have been corrected. Either the CBI or the vendor may discontinue service upon thirty days' advance written notice.

This agreement remains separate from all contracts between the CJIS Vendor and CGAs. Issues which may arise between the Vendor and the CGA shall be resolved between the contract parties.

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.

| | |
|---------------------------|--|
| Business Name and Address | |
|---------------------------|--|

| | | |
|-----------------------|------------------------|------|
| Vendor Representative | Title and Printed Name | Date |
|-----------------------|------------------------|------|

| | | |
|---------------------------------------|------------------------|------|
| Contracted Services Coordinator (CSC) | Title and Printed Name | Date |
|---------------------------------------|------------------------|------|

| | | |
|-----------------------|------------------------|------|
| CBI Director/Designee | Title and Printed Name | Date |
|-----------------------|------------------------|------|

Once signed, return this page to:

MAIL
CBI Vendor Management Program
690 Kipling Street Suite 3000 Denver,
CO 80215

FAX
(303) 239-5858

EMAIL
cdps_cbi_ident_taqc@state.co.us