MANAGEMENT CONTROL AGREEMENT
REGARDING
COLORADO BUREAU OF INVESTIGATION AND FBI
CRIMINAL JUSTICE INFORMATION SYSTEMS

The purpose of this document is to establish and enforce Security Control of the access and use of the Colorado Bureau of Investigation's (CBI) Colorado Crime Information Center (CCIC) database and associated CJIS systems (NCIC, Nlets, etc.) in a location where access to and/or use of that system is accomplished by a criminal justice agency with the assistance of a non-criminal justice governmental agency. This document places Security Control of that access and use under the authority of the criminal justice agency.

This document is an agreement between

_____

the "criminal justice agency," and,

_____

the "non-criminal justice agency" providing services in support of the criminal justice agency in the execution of its duties under the "administration of criminal justice."

Whereas the non-criminal justice agency manages the associated computer and/or equipment and personnel that provide the criminal justice agencies with access to CCIC and associated CJIS systems, and

Whereas the non-criminal justice agency through the Communications Supervisor performs certain functions of the Colorado Crime Information Center (CCIC) and the National Crime Information Center (NCIC) for the criminal justice agency, and

Whereas the criminal justice agency has signed an agreement with the Colorado Bureau of Investigation to use and participate in the state's telecommunications networks and associated systems, and

Whereas the state transmits state and national criminal history information over those networks, and

Whereas the state participates in the FBI CJIS Systems which require that all access to the FBI CJIS Systems be controlled by the *FBI CJIS Security Policy*, and

Whereas the CJIS Security Policy requires that the State CJIS Systems Agency (CSA) (i.e., the Colorado Bureau of Investigation) establish "Security Control," for that access, and

Whereas Security Control is defined as the ability of the CSA or criminal justice agency to set, maintain, and enforce:

1. Standards for the selection, supervision, and termination of personnel; and
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CJIS systems used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Whereas the Colorado Bureau of Investigation defines management control as the authority and responsibility to enforce Security Control as herein defined,

Therefore, be it resolved that this agreement hereby places the technical services division under the management control, as herein defined, of the criminal justice agency.

SECURITY

The non-criminal justice agency agrees to abide by all current and hereafter approved rules of the Colorado Bureau of Investigation and Federal Bureau of Investigation, including but not limited to all requirements of the *CJIS Security Policy*. The compliance with those requirements shall be determined by the criminal justice agency and the CBI.

Computers having access to CCIC/NCIC must have the proper software and hardware controls, implemented under the supervision of the criminal justice agency, to prevent criminal history and other CJIS data from being accessible to any terminals other than authorized terminals.

The non-criminal justice agency must allow adequate physical security, as required by the *CJIS Security Policy* and determined by the criminal justice agency, to protect against any unauthorized personnel gaining access to the terminals, computer equipment, or any of the stored data.

Personnel at the criminal justice agency site, or with remote access to the criminal justice agency's data, must be screened thoroughly under the authority and supervision of the criminal justice agency, in accordance with CCIC/NCIC policy. This screening applies to criminal justice and non-criminal justice personnel, including non-criminal justice maintenance and technical personnel. This screening will be done under the guidelines established in the *CJIS Security Policy*. Decisions by the criminal justice agency related to personnel are limited to the inclusion or exclusion of personnel from the criminal justice agency, according to the guidelines established by the CJIS Security Policy and implemented by CCIC Policy.

All visitors to the criminal justice agency and the technical services division must be accompanied by staff personnel at all times.

All terminals and network equipment having access to the state's law enforcement networks must be physically placed in secure locations, as required by the *CJIS Security Policy* and determined by the criminal justice agency.

Access to all terminals and network equipment that protects and/or transmits the criminal justice data must be restricted to the minimum number of authorized employees needed to complete the work.

Printed copies of criminal history data obtained from CCIC/NCIC must be afforded security to prevent any unauthorized access to or use of the data. When the printout is no longer needed, it must be filed in a secure file or destroyed.

No dial-up access will be permitted to a computer or a terminal with access to the state's law enforcement network unless that dial-up access has been approved by the criminal justice agency and the state.

No terminal will access the state's law enforcement networks, and no data will be requested or obtained through these networks without the approval of the criminal justice agency.

No changes will be made to the configuration of the networks accessing the state's law enforcement network without prior approval of the state.

TRAINING

Personnel at the criminal justice agency site, or with remote access to the criminal justice agency's data, must take Security Awareness training within 6 months of initial assignment, and biennially thereafter, as required by the *CJIS Security Policy*. This training and certification applies to criminal justice and non-criminal justice personnel, including non-criminal justice maintenance and technical personnel. This training shall include, at a minimum, the topics required by the *CJIS Security Policy*.

MONITORING AND AUDITING

The non-criminal justice agency agrees to allow the criminal justice agency and CBI necessary access, as determined by CBI and the criminal justice agency, to the physical locations, any computer programs, any computer files, and/or network activities necessary to implement and enforce security control as defined by the *CJIS Security Policy.* The criminal justice agency, in accordance with CCIC/NCIC policy, has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the non-criminal justice agency.

CBI and FBI audits of the technical services division will be to determine whether policies have been established by the criminal justice agency and implemented by the non criminal justice agency.

GENERAL

The criminal justice agency will not manage the day to day operations of the technical services division, but may establish and enforce the priorities necessary to meet CBI and FBI policies regarding system use.

The non-criminal justice agency agrees to cooperate with the criminal justice agency in the implementation of this agreement, and to accomplish the directives of the criminal justice agency under the provisions of this agreement.

Non-Criminal Justice Agency	**Criminal Justice Agency**
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date
Signature	Signature
	Printed Name
Title	Title
Date	Date

APPENDIX A

Appropriate environmental security measures would include:

a) A back-up power supply or uninterruptible power source.
b) Environment monitors and controls for temperature, air conditioning, humidity, etc.
c) Emergency lighting.
d) Adequate fire detection/suppression devices.
e) Emergency shutdown of system and/or power devices.
f) Duplicate computer files, if applicable, (as a countermeasure for unauthorized destruction of original files) which are to be maintained off premise. Computer tapes or discs should be locked in a safe (fireproof) storage area under the control of senior agency personnel. Secondary storage (off-site location) will be used to back-up.

APPENDIX B

The standards apply to all personnel with access to network systems as defined in Title 28 CFR, Part 20 to CHRI data, including, but not limited to:

a) Management personnel who direct criminal justice related software, hardware, or dispatch functions.
b) Supervisory personnel who supervise criminal justice related software, hardware, or dispatch functions; or have terminal access to criminal justice data either directly or through their subordinates; or who have general responsibility for criminal justice related data storage, switching, transmission and logging.
c) Personnel involved in analysis, evaluation and/or programming of criminal justice related data stored, switches, transmitted or logged by the center.
d) Non-Data processing personnel who regularly provide necessary software or hardware installation, modification or maintenance in the dispatch center.
e) Non-Data Processing personnel who provide temporary and necessary software, hardware or telecommunications installation, modification or maintenance, or such other services as deemed necessary by the Communications Supervisor.
f) All other persons with direct access to the dispatch center or terminals with access to the state’s telecommunications system.