FOIA EXEMPTION:7(1)(v)-Security Plans

SOP Number: 5.01

BLOOMINGTON POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

POLICE DEPARTMENT SECURITY

Reviewed by: Asst. Chief Kenneth Bays		Effective Date: March 15, 1999
Authorized by: Chief Brendan O. Heffner		Revision Date: December 9, 2015

PURPOSE

The purpose of this policy is to promote security for citizens, department personnel, the physical police building, and the physical protection of Criminal Justice Information (CJI).

This Security Policy was developed using the FBI's CJIS Security Policy 5.1 dated July 13, 2012.

DEFINITIONS

Physically secure location is a facility, an area, a room, or a group of rooms within a facility with both physical and personnel security controls sufficient to regulate access and provide security for facility personnel and Criminal Justice Information (CJI) and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted areas in Bloomington Police Department (BPD) facilities shall be identified with a sign bearing the word "RESTRICTED" at the entrance.

Local area security officer (LASO) means a department employee(s) tasked with monitoring compliance with established security protocols.

Escort means a Sworn law enforcement officer accompanying victims, witnesses, and suspects, as defined by this policy, while in restricted areas of the BPD facility; or any BPD employee accompanying visitors as defined in this policy, while in restricted areas of the BPD facility

Colored lanyards indicate access levels

1. BLUE LANYARD WITH PICTURE AND NAME ID BADGE indicate
    a. Bearer is a BPD employee or works primarily out of the BPD building
    b. Does not require an escort

2. GREEN LANYARD ID BADGE WITH PICTURE AND NAME indicates
    a. Bearer is support personnel employed outside of BPD
        i. Employed by the city
        ii. Employed by a contracted support company
    b. Bearer is not required to be escorted while in restricted areas of the BPD building.

3. RED LANYARD WITH ID BADGE BEARING "VISITOR" indicates

a. Bearer is a visitor
b. Bearer **must** be escorted by a BPD employee at **all times** while in restricted areas of a BPD facility

Only department issued lanyards are to be used

Access log is a log book maintained at the CSO desk where required individuals sign in and out of the department by an approved department employee.

Non visitors

1. Approved Individuals
    a. Those working full time in the BPD building (BLUE LANYARD)
        i. Direct employee of BPD
        ii. Intern of BPD
        iii. Non city employees assigned a workstation in the restricted areas of the police facility (eg. parole officer, domestic violence advocate)
    b. Other specified city support personnel (GREEN LANYARD)
        i. Designated support personnel from other city departments
        ii. Information Services
        iii. Facilities Management
        iv. Fleet Mechanics
        v. Access status
            1. Name, picture, and department in Access Log book
            2. Maintained and updated by LASO(s) quarterly
    c. Access requirements
        i. Not required to sign in on Access Log
        ii. Do not require an escort
        iii. Possess a BPD key card
        iv. Non-sworn personnel will wear an appropriately colored lanyard attached to their city issued photo ID when working in the BPD building.
        v. Sworn BPD personnel not wearing a uniform or displaying a law enforcement badge shall wear an appropriately colored lanyard attached to their city issued photo ID
        vi. Sworn BPD personnel in uniform or displaying a law enforcement badge are not required to wear a lanyard or ID Badge
        vii. Sworn BPD personnel assigned to work in an undercover capacity are exempt from displaying an ID or lanyard
        viii. Employees utilizing the department work-out room, shall not wear a lanyard while using the work-out room; ID should be readily accessible
        ix. Employees arriving or departing work do not need to display their lanyard provided they are going directly to or from their work station or locker room as they arrive or depart. Once arriving at their work station, those required to display their lanyard shall do so.

2. Non BPD Law Enforcement officers (local, state, and federal)
    a. Uniformed sworn officers do not need to sign in or be escorted
    b. Sworn Officers displaying a badge do not need to sign in or be escorted

- c. Sworn personnel assigned to work in an undercover capacity are exempt from displaying an ID or lanyard but shall be accompanied by BPD personnel when in restricted areas
- d. Sworn Officers not in uniform and not displaying a badge are required to sign in as a VISITOR and are to be escorted at all times by a BPD employee while in restricted areas of the BPD building

3. Contractors (BPD issued GREEN LANYARD)
   - a. Not employed by the City of Bloomington
   - b. Provide support services to the police department (eg. Radio service personnel)
   - c. Access Status
     - i. Name, picture, and company listed in Access Log book
     - ii. Maintained and updated by LASO(s) quarterly
   - d. Access requirements
     - i. Required to sign in and out (see sign in procedures)
     - ii. Present company ID and government issued picture ID
     - iii. Obtain at sign in
       1. GREEN lanyard with ID badge reading "CONTRACTOR", bearer's name, company, and picture to be worn and visible at all times while in the restricted areas of the BPD building
       2. BPD key card if applicable
   - e. Do not require an escort while in restricted areas of the BPD building
   - f. Return ID badge and BPD key card upon signing out

4. Arrestees, suspects, witnesses, and victims (NO LANYARD)
   - a. Not required to sign in
   - b. <u>**Must**</u> be escorted by BPD SWORN personnel at <u>**all times**</u> while in restricted areas of the BPD building, excluding interview rooms

Visitors (RED LANYARD)

1. Any individual not meeting the definition of NON VISITORS
   - a. Employee family members (16 y.o.a. or over)
   - b. Vendors or other service personnel (vending machines, rug delivery, etc.)
   - c. All others
2. Access requirements
   - a. Must follow sign in procedures
   - b. Obtain at sign in a RED lanyard with ID badge reading "VISITOR" to be worn and visible at all times while in the restricted areas of a BPD building
   - c. Require an escort at all times while accessing restricted areas of the BPD building
   - d. Return lanyard with ID badge at sign out.

SIGN IN AND SIGN OUT PROCEDURES

Visitors and Contractors must

1. Present Bloomington Police Department personnel a valid government issued photo identification (ID) and company ID for Contractors. Entry may be granted without photo ID if the subject is personally known to the police department employee overseeing the sign in process or other BPD personnel present at the time of check in.

2. Provide information for the Access Log located at the CSO Desk. Information for the log which will include:
    a. Date of visit,
    b. Visitor Badge ID #
    c. Issued key card number (if applicable)
    d. Time of arrival
    e. Name
    f. Visitor’s company (if applicable)
    g. Name of personnel to be visited.
3. Obtain the appropriate colored lanyard, ID badge, and BPD key card if applicable
4. Display the visitor or contractor badge at all times by wearing on the visitor’s or contractor's outer clothing
5. Conclusion of visit
    a. Return ID Badge and lanyard
    b. Return key card (if applicable)
    c. Sign out and collected by the end of the agency at the end of the visit.

REQUIREMENTS FOR INDIVIDUALS ACCESSING RESTRICTED AREAS OF THE BPD BUILDING

Individuals meeting the definition of VISITOR will be accompanied by a Bloomington Police Department employee escort at all times to include delivery or service personnel. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Bloomington Police Department policy for non BPD employees with authorized unescorted access

1. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement (SEE APPENDIX A) between the Bloomington Police Department and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
2. Private contractors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum (SEE APPENDIX B) between the Bloomington Police Department and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

Are not allowed to view screen information.

Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel are to be notified or call 911.

Not be allowed to sponsor another visitor.

All requests by groups for tours of the Bloomington Police Department facility will be referred to the proper agency point of contact for scheduling. The department employee conducting the tour will keep the group together and escorted at all times. In most cases, these groups will be handled by a single form kept in the Access Log Book (SEE APPENDIX C), to be signed by a designated group leader or representative. The number of adults and juveniles in the group will also be recorded on the form. Each member of the group will be provided a "VISITOR" sticker to be affixed in a visible location on their person. The department employee conducting the tour will complete any additional information required on the form and insert the form in the Access Log Book at the beginning of the tour. Remaining visitor rules apply for each visitor within the group.

At no time will a key card or key fob be kept with or attached to the issued lanyard and ID.

WEAPONS

Only sworn law enforcement officers may possess firearms while in any BPD facility.

According to the Rules and Regulations of the Bloomington Police Department, officers will be armed at all times while on duty.

Officers will not enter into a detention room or secured room where a suspect or arrested person is being held without first securing their weapons in the weapons lockers provided. This includes representatives of other police or military agencies. Compliance with this policy is the duty of the assisting Bloomington Police officer.

At no time will any weapon be left unattended in the Bloomington Police facility, unless deposited in a locked receptacle.

Appendix A

Interagency Agreement
Criminal Justice Agency and
Noncriminal Justice/Private Contractor

This document is an agreement between the ________________________________, a criminal justice agency, and the ____, a noncriminal justice/private contractor. This agreement is established for the purpose of the noncriminal justice/private contractor providing the administration of criminal justice service to the criminal justice agency *(attach to this agreement a description of criminal justice service being provided)*

WHEREAS, various statutes, regulations and rules require that certain conditions be met to ensure the privacy and security of LEADS and NCIC; and

WHEREAS, the criminal justice agency, transmits state and national criminal history information over the LEADS network; and

WHEREAS, Illinois LEADS agencies participate in the National Crime Information Center, which requires compliance to security policy established under 28 CFR 20.33; and

WHEREAS, noncriminal justice/private contractor entities are sometimes tasked to provide services to a criminal justice agency in support of a criminal justice function.

THEREFORE, be it resolved that this agreement hereby affirms the commitment of the noncriminal justice/private contractor, to adhere to the FBI Criminal Justice Information Services (CJIS) Security Addendum (attached) governing the security for all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

The noncriminal justice/private contractor accessing LEADS/NCIC data will be subject to all operational policies, rules and regulations. Security and management control responsibility must remain with the criminal justice agency. (LEADS Administrative Rules, Section 1240.30 - c and FBI Security Policy, Administrative Security, Noncriminal Justice [LEADS 2000 client, LEADS Information, Security]).

Employees of the noncriminal justice/private contractor who have direct access to computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support the telecommunications network through which LEADS/NCIC criminal justice data is being accessed, must be screened thoroughly (including an state of residence and federal fingerprint-based records check) under the authority and supervision of the criminal justice agency in accordance with LEADS and NCIC policy. This screening applies to criminal justice and noncriminal justice/private contractor personnel. This screening will be done in accordance with the guidelines established in the LEADS Security Policy and under the management control of the criminal justice agency.

IN WITNESS WHEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

CRIMINAL JUSTICE AGENCY	**NONCRIMINAL JUSTICE/PRIVATE CONTRACTOR**
____________________ Agency Head	____________________ Agency Head
____________________ Agency Head Title	____________________ Agency Head Title
__________ Date	__________ Date

R - 05/10/07

Appendix B

Federal Bureau of Investigation
Criminal Justice Information Services
Security Addendum

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform and Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statue also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

Appendix B

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

Appendix B

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

Appendix B

Federal Bureau of Investigation
Criminal Justice Information Services
Security Addendum

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the surety and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CJA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature as defined in the CJIS Security Policy.

3.00 Responsibilities of the Contractor.

Appendix B

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent version), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

Appendix B

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Appendix B

Federal Bureau of Investigation
Criminal Justice Information Services
Security Addendum

Certification

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; acing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_______________________________ _______________
Printed Name/Signature of Contractor Employee Date

_______________________________ _______________
Printed Name/Signature of Contractor Representative Date

____
Organization and Title of Contractor Representative

APPENDIX C

BLOOMINGTON POLICE DEPARTMENT GROUP ACCESS FORM

Date:________________

Time:________________

Organization Name:____

Designated Group Leader's Name:

_______________________________Printed

_______________________________Signature

Number of Adults:__________

Number of Juveniles:________

Other Comments if needed:

City Employee escorting the group:
Signature/ID# _____________________________________/____________