

WISCONSIN DEPARTMENT OF JUSTICE
CRIME INFORMATION BUREAU

MANAGEMENT CONTROL AGREEMENT

Between

OPERATING AGENCY _____
(Noncriminal Justice Agency)

and

USER AGENCY _____
(Criminal Justice Agency)

PURPOSE: This agreement is intended to establish the minimum required oversight of the USER AGENCY over the OPERATING AGENCY which operates the interface with TIME/NCIC.

SCOPE: The use of all computers, electronic switches, and manual terminals interfaced directly with the TIME/NCIC computer must be under the oversight control of criminal justice agencies. This control includes, but is not limited to the supervision of staff, equipment, systems design, programming, and the operation of the interface to TIME/NCIC by the OPERATING AGENCY.

Pursuant to the above Purpose and Scope of requirements established by the Wisconsin Department of Justice, Crime Information Bureau (CIB) and the National Crime Information Center (NCIC), Federal Bureau of Investigation, the OPERATING AGENCY and the USER AGENCY agree to the following:

1. USER AGENCY shall have control over the interface to the TIME/NCIC computer which is organizationally located within the OPERATING AGENCY.
2. USER AGENCY shall have direct management input into:
 - a. The priority of service provided to USER AGENCY by OPERATING AGENCY.
 - b. The standards for selection, supervision, assignment, and removal of personnel employed by OPERATING AGENCY to manage, supervise, or operate the interface to the TIME/NCIC computer.
 - c. Policy covering the selection, maintenance, and separation of that portion of the equipment used by OPERATING AGENCY to store, process, and transmit data to/from the TIME/NCIC computer.
3. USER AGENCY has the right to initiate administrative action leading to the transfer or removal of personnel authorized direct access to the TIME/NCIC interface when such personnel violate TIME/NCIC operating or security rules or regulations.

Management Control Agreement & Security Addendum

4. OPERATING AGENCY agrees that USER AGENCY shall have the authority to perform the following:
 - a. Conduct background screening and reject consistent with 111.335 Wisconsin Statute and the CJIS Security Policy for employment of all personnel to be authorized to have direct access to criminal history record information or the TIME/NCIC interface.
 - b. Audit, monitor, and inspect all operations of the operating agency computer center and/or communications center which are related to the operation of the interfaces to the TIME/NCIC computer.
 - c. Set the appropriate security standards for the operating agency computer center and/or communication center.
5. OPERATING AGENCY and USER AGENCY agree to jointly operate the interface to the TIME/NCIC computer within the policies and standard procedures published by TIME/NCIC, all current state and federal laws or regulations and the attached Security Addendum.
6. OPERATING AGENCY agrees to notify USER AGENCY and CIB of any change in the services provided by or agencies serviced by the operating agency computer center and/or communications center from those intact at the time of the agreement.
7. OPERATING AGENCY agrees to provide all employees with access to the TIME/NCIC interface a copy of the attached Security Addendum. Each of these employees will be required to sign the Security Addendum certification. The OPERATING AGENCY representative will sign each certification form and return to the USER AGENCY who will maintain possession for audit purposes.

WE, THE UNDERSIGNED PARTIES, AGREE TO THE ABOVE PURPOSE, PRINCIPLES, AND STANDARDS OF MANAGEMENT CONTROL AND RESPONSIBILITY.

Operating Agency Head

User Agency Head

(Signature / Date)

(Signature / Date)

&

(Title)

(Title)

(Typed/Printed Name)

(Typed/Printed Name)

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

The goal of this document is to provide adequate security for criminal justice systems while under the control or management of a private entity, the 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 security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security and data 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 Administration of criminal justice - the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment.
- 1.02 Agency Coordinator (AC) - a staff member of the Contracting Government Agency, who manages the agreement between the Contractor and agency.
- 1.03 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 contractor subject to this Security Addendum.
- 1.04 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.
- 1.05 Control Terminal Agency (CTA)- a duly authorized state or federal criminal justice agency with direct access to the National Crime Information Center (NCIC) telecommunications network providing statewide (or equivalent) service to its criminal justice users with respect to the various systems managed by the FBI CJIS Division.
- 1.06 Control Terminal Officer (CTO)- an individual located within the CTA responsible for the administration of the CJIS network for the CTA.
- 1.07 Criminal Justice Agency (CJA)- The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

- 1.08 Noncriminal Justice Agency (NCJA) - a governmental agency or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.
- 1.09 Noncriminal justice purpose - the uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.10 Security Addendum - a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

2.00 Responsibilities of the Contracting Government Agency

- 2.01 The CGA entering into an agreement with a Contractor is to appoint an AC.
- 2.02 In instances in which responsibility for a criminal justice system has been delegated by a CJA to a NCJA, which has in turn entered into an agreement with a Contractor, the CJA is to appoint an Agency Liaison to coordinate activities between the CJA and the NCJA and Contractor. The Agency Liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the NCJA's authority is directly from the CTA, there is no requirement for the appointment of an Agency Liaison.
- 2.03 The AC will be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of certification testing and all required reports by NCIC.
- 2.04 The AC has the following responsibilities:
 - a. Understand the communications and records capabilities and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA;
 - b. Participate in related meetings and provide input and comments for system improvement;
 - c. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees;
 - d. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor;
 - e. Maintain up-to-date records of employees of the Contractor who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date certified or recertified (if applicable);
 - f. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for a certification exam with the CTA staff. Schedule new operators for the certification exam within six (6) months of employment. Schedule certified operators for re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for any other mandated class;
 - g. The AC will not permit an un-certified employee of the Contractor to access an NCIC terminal;

- h. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements;
 - i. Provide completed Applicant Fingerprint Cards on each person within the Contractor who accesses the System to the CJA (or, where appropriate, CTA) for criminal background investigation prior to such employee accessing the system; and
 - j. Any other responsibility for the AC promulgated by the FBI.
- 2.05 The CTA shall ensure that all NCIC hot file transactions and Interstate Identification Index (III) transactions be maintained on an automated log for a minimum of six months. This automated log must identify the operator on III transactions, the agency authorizing the transactions, the requester, and any secondary recipient. This information can be captured at log on and can be a name, badge number, serial number, or other unique number.

3.00 Responsibilities of the Contractor

- 3.01 The Contractor shall maintain a security program which complies with this Security Addendum.
- 3.02 The Contractor shall assign a Security Officer accountable for the management of this security program. This person shall coordinate with the CGA to establish the security program.
- 3.03 The Contractor shall document the security program in a Security Plan. The Security Plan shall describe the implementation of the security requirements described in this Security Addendum, the associated training program, and the reporting guidelines for documenting and communicating security violations to the CGA. The Security Plan shall be subject to the approval of the CJA, even in instances in which the CGA is the NCJA.
- 3.04 The Contractor shall provide for a Security Training Program for all Contractor personnel engaged in the management, development, operation, and/or maintenance of criminal justice systems and facilities. Annual refresher training shall also be provided.
- 3.05 The Contractor shall establish a security violation response and reporting procedure to discover, investigate, document, and report on all security violations. Violations which endanger the security or integrity of the criminal justice system or records located therein must be communicated to the CGA immediately. Minor violations shall be reported to the CGA on a periodic basis, but in no instance less than quarterly. See Section 8.01.
- 3.06 The Contractor's facilities will be subject to unannounced security inspections performed by the CGA. These facilities are also subject to periodic FBI and state audits.
- 3.07 The security plan is subject to annual review by the CJA and the Contractor. During this review, efforts will be made to update the program in response to security violations, changes in policies and standards, and/or changes in federal and state law and technology.
- 3.08 The Contractor and its employees will comply with all federal and state laws, rules, procedures and policies (including the CJIS Security Policy in effect when the contract is executed) formally adopted by the FBI and the CJIS APB, including those governing criminal history record information.

4.00 Site Security

- 4.01 The Contractor shall dedicate and maintain control of the facilities, or areas of facilities, that support the CGA.

- 4.02 All terminals physically or logically connected to the computer system accessing NCIC and the criminal justice files must be segregated and screened against unauthorized use or observation.

5.00 System Integrity

- 5.01 Only employees of the Contractor, employees of CGA, the Agency Liaison, and such other persons as may be granted authorization by the CGA shall be permitted access to the system.
- 5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.
- 5.03 Access to the system shall be available only for official purposes consistent with the appended Agreement. Any dissemination of NCIC data to authorized employees of the Contractor is to be for their official purposes.
- 5.04 Information contained in or about the system will not be provided to agencies other than the CGA or another entity which is specifically designated in the contract.
- 5.05 All criminal history record information requests must be envisioned and authorized by the appended Agreement. A current up-to-date log concerning access and dissemination of criminal history record information shall be maintained at all times by the Contractor.
- 5.06 The Contractor will ensure that its inquiries of NCIC and any subsequent dissemination conforms with applicable FBI/NCIC policies and regulations, as set forth in (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the Policy and Reference Manual; (4) the CJIS Security Policy; and (5) Title 28, Code of Federal Regulations, Part 20. All disseminations will be considered as "Unclassified, For Official Use Only."
- 5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the criminal justice information system. In no event shall copies of messages or criminal history record information be disseminated other than as envisioned and governed by the appended Agreement.

6.00 Personnel Security

- 6.01 Appropriate background investigations must be conducted on all Contractor employees and the Contractor's vendors which provide system maintenance support.
- 6.02 Thorough background screening by the CGA is required. This investigation includes submission of a completed applicant fingerprint card to the FBI through the state identification bureau. State and national record checks by fingerprint identification must be conducted for all personnel who manage, operate, develop, access and maintain criminal justice systems and facilities. Record checks must be completed prior to employment.
- 6.03 When a request is received by the CTA before system access is granted:
- a. The CGA on whose behalf the Contractor is retained must check state and national arrest and fugitive files. These checks are to be no less stringent than those performed on CJA personnel with access to NCIC.
 - b. If a record of any kind is found, the CGA will be formally notified, and system access will be delayed pending review of the criminal history record information. The CGA will in turn notify the Contractor-appointed Security Officer.

- c. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA's designee will review the matter. A Contractor employee found to have a criminal record consisting of any felony convictions or of misdemeanor offenses which constitute a general disregard for the law is disqualified. Applicants shall also be disqualified on the basis on confirmations that arrest warrants are outstanding for such applicants.
 - d. If an adverse employment determination is made, access will be denied and the Contractor-appointed Security Officer will be notified in writing of the access denial. This applicant will not be permitted to work on the contract with the CGA. Disqualified employees and applicants for employment shall be notified of the adverse decisions and the impact that such records had on such decisions.
- 6.04 The investigation of the applicant's background shall also include contacting of employers (past or present) and personal references.
- 6.05 The Security Officer shall maintain a list of personnel who successfully completed the background investigation.
- 6.06 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum 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.
- 6.07 The CGA shall ensure that each Contractor employee authorized to access CJIS network terminals or information provided therefrom is specially trained in the state and federal laws and rules governing the security and integrity of criminal justice information.
- 6.08 All visitors to sensitive areas of Contractor facilities must be escorted at all times by a Contractor employee with clearance. Names of all visitors shall be recorded in a visitor log, to include date and time of visit, name of visitor, purpose of visit, name of person visiting, and date and time of departure. The visitor logs shall be maintained for five years following the termination of the contract.

7.00 System Security

- 7.01 Transmission, processing, and storage of CJA information shall be conducted on dedicated systems. Increased reliance should be placed on technical measures to support the ability to identify and account for all activities on a system and to preserve system integrity.
- 7.02 The system shall include the following technical security measures:
- a. unique identification and authentication for all interactive sessions;
 - b. if warranted by the nature of the contract, advanced authentication techniques in the form of digital signatures and certificates, biometric or encryption for remote communications;
 - c. security audit capability for interactive sessions and transaction based logging for message-based sessions; this audit shall be enabled at the system and application level;
 - d. access control mechanisms to enable access to be restricted by object (e.g., data set, volumes, files, records) to include the ability to read, write, or delete the objects;
 - e. ORI identification and access control restrictions for message based access;
 - f. system and data integrity controls;

g. access controls on communications devices;

h. confidentiality controls (e.g., partitioned drives, encryption, and object reuse).

7.03 Data encryption shall be required throughout the network passing through a shared public carrier network.

7.04 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

7.05 The Contractor shall establish a procedure for sanitizing all fixed storage media (e.g., disks, drives) at the completion of the contract and/or before it is returned for maintenance, disposal or reuse. Sanitation procedures include overwriting the media and/or degaussing the media. If media cannot be successfully sanitized it must be returned to the CGA or destroyed.

8.00 Security violations

8.01 Consistent with Section 3.05, the Contractor agrees to inform the CGA of system violations. The Contractor further agrees to immediately remove any employee from assignments covered by this contract for security violations pending investigation. Any violation of system discipline or operational policies related to system discipline are grounds for termination, which shall be immediately reported to the AC in writing.

8.02 The CGA must report security violations to the CTO and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

8.03 Security violations can justify termination of the appended agreement.

8.04 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 the actual NCIC telecommunications link. The FBI will provide the CTO 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 CJA and Contractor. Upon termination, the Contractor's records containing criminal history record information must be deleted or returned to the CGA.

8.05 The FBI reserves the right to audit the Contractor's operations and procedures at scheduled or unscheduled times. The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

9.00 Miscellaneous provisions

9.01 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), CTA, and FBI.

9.02 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 Policy and Reference Manual; (4) the CJIS Security Policy; and (5) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

Management Control Agreement & Security Addendum

- 9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- 9.04 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.
- 9.05 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

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I have read and am familiar with the contents of (1) the Security Addendum; (2) the TIME 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; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or redisseminating 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 redisseminating 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.

Signature of Contractor Employee

Date

Signature of Contractor Representative

Date

Organization and Title