WISCONSIN DEPARTMENT OF JUSTICE
CRIME INFORMATION BUREAU

MANAGEMENT CONTROL AGREEMENT

Between

Operating Agency: _____

User Access 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.
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 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 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, 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 (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.

1.02 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 (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

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 versions), 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.

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

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; accessing 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