



BILL HASLAM
Governor

TENNESSEE BUREAU OF INVESTIGATION
 901 R.S. Gass Boulevard
 Nashville, Tennessee 37216-2639
 (615) 744-4000
 TDD (615) 744-4001



MARK GWYN
Director

TENNESSEE INFORMATION ENFORCEMENT SYSTEM
VENDOR USER AGREEMENT

This agreement is made and entered into between the Tennessee Bureau of Investigation (TBI), a department of government of the State of Tennessee and _____, referred to herein as the Vendor, to be effective on the date hereafter provided.

The Tennessee Bureau of Investigation, administering the Tennessee Crime Information Center (TCIC), pursuant to the laws of Tennessee including Chapter 10 of Title 38 and a written agreement between the TBI for the State of Tennessee and the Department of Justice for the United States Government, agrees to provide available criminal justice-related information and/or interfaces for the transmission and/or retrieval of said information, subject to the following provisions:

The vendor must have a specific agreement / contract with each criminal justice agency for which it provides services for the administration of criminal justice, to include criminal justice dispatching functions or data processing/information services for the criminal justice agency or agencies to access the Tennessee Information Enforcement System (TIES) network. Pursuant to the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, the agreement between the vendor and the criminal justice agency must incorporate the CJIS Security Addendum approved by the Director of the FBI (acting for the U. S. Attorney General), as referenced in Title 28 CFR 20.33 (a)(7). The security addendum specifically authorizes access to criminal history record information and criminal justice information, limits the use of the information to the specific purposes for which it is provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, and the CJIS Security Policy provides for sanctions, and contains such other provisions as the Attorney General may require.

The TBI, the CJIS Systems Agency (CSA) in Tennessee, will provide the vendor with such access to the TIES network as needed by the vendor for the performance of its duties, pursuant to the provisions of the agreement with the criminal justice agency for which it provides services. Such access by the vendor shall be in compliance with the CJIS Security Policy, as amended, and the rules, regulations, policies, and procedures promulgated by the TBI, the National Crime Information Center (NCIC), and the International Justice and Public Safety Network (NIJ), relating to the operation of these networks and the acquirement, transmission, use and dissemination of criminal justice information available for these networks.

If the vendor provides a workstation or software interface application for the criminal justice agencies to utilize the TIES network, to include sending and receiving images when applicable, the vendor must ensure that the application is kept up to date with current



INTERNATIONALLY ACCREDITED SINCE 1994

functions and requirements. The vendor and its product must also have been approved by TBI.

The vendor agrees that use of the TIES network will be strictly limited to the administration of criminal justice support functions of the vendor. Under no circumstances shall criminal justice information be disseminated further. Remote access is only allowed for technical support. The vendor must not unlawfully access the TIES network/data for any other reason. The use of any remote access software is permitted only for the purpose of providing technical support to the private network or individual TIES devices. Furthermore, any software used to remotely access criminal justice computer systems, whether for maintenance, repair, or any other purpose, must be implemented in such a manner as to provide for the following:

- A. No connection shall be made without operator intervention to allow the connection. This can be achieved in any manner applicable to the software being used, but shall not allow access without an operator manually enabling it;
- B. Any person accessing the criminal justice system must have his/her own unique ID for connecting to the device via the remote control software;
- C. Passwords for accessing the criminal justice system must meet the CJIS standards for passwords; and,
- D. All connections must be logged with date, time, ID of remote user, and duration of the connection.

Through the supported agency, the vendor must submit to TBI, for review and approval, written documentation describing the use of remote access software, and the security measures that will be implemented to ensure the integrity of the TIES network/data, prior to installing any type of remote control access software on the private network or the TIES devices.

The vendor must not add additional TIES network accessible devices without TBI approval, through the supported agency. TIES network access must be limited to devices approved by TBI. The vendor shall be responsible for all maintenance/diagnostics beyond the connectivity point provided by the TBI. Since public safety and criminal justice operations are critical to the lives, safety, and property of citizens, the vendor must provide the highest operational support priority to the criminal justice devices serviced by the vendor. Other applications must not interfere with the delivery of criminal justice messages. The vendor shall familiarize the agency with the hardware, software, boot-up procedures and error messages. The vendor must configure the device software as specified by the TBI.

The vendor shall advise its employees of the penalties for misuse of criminal justice information. The vendor's employees, who manage, operate, develop, access and maintain criminal justice systems, shall be subject to background investigations as prescribed by the TBI and the FBI, which include the submission of applicant fingerprint cards. In addition, all applicable vendor employees shall read the CJIS security addendum and sign the certification form, which shall be appended to this agreement.

Nothing in this agreement shall be interpreted as giving authority to the vendor to invade the privacy of any citizen. The vendor agrees to immediately remove any employee from assignments covered by this contract for security violations, pending further investigation. In addition, any violation of system discipline or operational policies related to system discipline shall immediately be reported in writing to the TBI's Information Security Officer.

The TBI reserves the right to terminate this agreement, with or without notice, upon determining that the vendor has violated terms of this agreement and/or the rules, regulations, policies and procedures of TBI, TIES, FBI, NCIC, or Nlets.

Vendor:

Authorized Representative (Printed Name / Signature)

Title

Date

Tennessee Bureau of Investigation:

Director

Date

CJIS Systems Officer

Date

**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 CJA 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 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.

Vendor Employee (Printed Name)

Vendor Employee (Signature)

Date

Vendor Representative (Signature)

Date

Title of Vendor Representative

Company Name