

**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 an 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 statute 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.

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:
 - 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.

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

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings
- [USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.6 – Agency User Agreements
 - c. 5.1.1.7 – Outsourcing Standards for Channelers*
 - d. 5.1.3 – Secondary Dissemination
 - e. 5.2.1.1 – All Personnel (Security Awareness Training)
 - f. 5.3 – Incident Response
 - g. 5.4 – Auditing and Accountability
 - h. 5.8 – Media Protection
 - i. 5.9.2 – Controlled Area
 - j. 5.11 – Formal Audits **
 - k. 5.12 – Personnel Security***

* Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

**Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

*** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication (web-site access)
 - c. 5.10.1.2 – System and Communications Protection – Encryption
4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity
5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
 - a. 5.7 – Configuration Management
 - b. 5.10 – System and Communications Protection and Information Integrity
6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance is directed toward those criminal justice agencies that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and, may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as “terminal agencies”. The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.3 – Criminal Justice Agency User Agreements
 - c. 5.1.3 – Secondary Dissemination
 - d. 5.2.1.1 – Security Awareness Training
 - e. 5.3 – Incident Response
 - f. 5.4.6 – Audit Record Retention
 - g. 5.8 – Media Protection
 - h. 5.9 – Physical Security
 - i. 5.10.2 – Facsimile Transmission of CJI
 - j. 5.11 – Formal Audits*
 - k. 5.12 – Personnel Security

*Note: States shall triennially audit all CJAs

2. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity