FBI CJIS SECURITY ADDENDUM

The following is an expanded version of the FBI Criminal Justice Information Services (CJIS) Security Addendum. This document was created in order to assist Texas agencies and their vendors in their compliance with the FBI CJIS Security Policy. The certification page is an acknowledgement, by the vendor and its individual employees, that they have read and understand the requirements contained within the referenced documents. All references are codified in the FBI CJIS Security Policy itself. Any questions regarding the Texas implementation of the FBI CJIS Security Addendum should be directed to the Crime Records Service at the Texas Department of Public Safety via telephone (512) 424-5686 or email to: Security.Committee@txdps.state.tx.us.

Agencies are urged, prior to the agency's entire packet submission to DPS, to perform a review of the contractor responses to the following Security Addendum requirements, as lack of completeness delays the DPS Security Review process, which in turn, can ultimately lead to the criminal justice agency's lack of connectivity to the TxDPS TLETS network. The responsibility for contractor compliance with the FBI requirements, and the enforcement thereof, resides with the criminal justice agency, with support from the TxDPS and the FBI.

In addition, a signature page has been added to gather the names of the parties who signed the original contract, and are therefore responsible for adherence to the agreed CJIS Security Addendum between the involved agencies/contracting firms.

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....
- (6) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
- (7) 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.

Note to the 3/2003 edition of Security Addendum:

Upon its creation in 10/1999, the Security Addendum obligated the contracting parties (and most particularly, the private entity) to abide by numerous federal laws, regulations, and (formal and informal) CJIS Division and CJIS Advisory Policy Board policies. Subsequently, the CJIS Security Policy, which contains many of the relevant portions of those sources, was developed. This compendium resulted in a new Certification being drafted, effective 1/10/2001, which replaced the citation to many of these authorities with the CJIS Security Policy, thereby providing a contracting party with a short and finite list of authorities with which to comply.

Although the Certification was updated, the body of the Security Addendum still contained the old authorities. Additionally, the CJIS Security Policy, which was formerly part of the Policy and Reference Manual, became a separate document. The 3/2003 edition coalesces the body of the Security Addendum (principally in Sections 5.06 and 9.02) with the Certification; it makes no substantive changes.

Note to the 5/2006 edition of the Security Addendum:

With the evolution of policies and procedures relevant to CJIS Systems, certain policy documentation must also periodically be updated. These modifications include an update in basic terminology as recently approved by the Advisory Policy Board to reflect references to "CJIS Systems" (replacing "NCIC"), and the "CJIS Systems Agency (CSA)" and "CJIS Systems Officer (CSO)", replacing Control Terminal Agency (CTA) and Control Terminal Officer (CTO), respectively. "Technical security" has been added to elements of a security program to be administered within the contractual relationship between the contracting governmental agency and the contractor. Clarifying language has been added: in Section 2.03 with regard to initial training, testing and certification of CJIS Systems operators; in Section 2.05 to reflect current policy regarding maintenance of dissemination_logs; in Sections 5.06, 9.02, and the Certification Page to delete references to the now obsolete Policy and Reference Manual; and in Section 603(d) to establish that in extenuating circumstances, the CSO may be requested by the contracting government agency to review adverse employment decisions. The Certification Page has also been modified to be consistent with the language in the CJIS Systems User Agreement, in that it now simply requires the signatory to "be familiar with" the contents of the listed authorities. This 5/2006 version should be used henceforth (until superceded) for outsourcing contracts.

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, 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 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 CJIS Systems Agency (CSA) a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.
- 1.06 CJIS Systems Officer (CSO) an individual located within the CJIS Systems Agency responsible for the administration of the CJIS network for the CJIS Systems Agency.
- 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.

Contracting Government Agency:
Criminal Justice Agency:
Contractor:
2.00 Responsibilities of the Contracting Government Agency
2.01 The CGA entering into an agreement with a Contractor is to appoint an AC.
AC Name:
Comments:
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 CSA, there is no requirement for the appointment of an Agency Liaison.
Agency Liaison Name:
Comments:

	_	sting and all required reports by NCIC.
Requi	ement m	et: Yes (See Plan in 2.04): No \[\]
Comm	ents:	
2.04	The A	C 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 initially trained, tested, certified or recertified (if applicable);
	f.	Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA_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 untrained/untested or non-certified employee of the Contractor to access a CJIS System;
	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, CSA) for criminal background investigation prior to such employee accessing the system; and
	j.	Any other responsibility for the AC promulgated by the FBI.
Requi	ement m	et: Yes, plan available for review: No
Plan s	ummary:	

The AC will be responsible for the supervision and integrity of the system, training and

2.03

for a minimum of six months and Interstate Identification Index (III) transactions be maintained on an automated log for a minimum of one year. This automated log must clearly identify the operator on III transactions, the authorized receiving agency, 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.			
This automated logging requirement is met by TxDPS for all Hot file and CCH/III transactions performed across the TLETS network. While DPS performs the automatic logging of each Hot File and CCH/III transaction, CCH/III logging for secondary dissemination is the local agency's responsibility. This CCH/III secondary dissemination logging requirement may be met either by electronic or manual means.			
Are CCH/III secondary dissemination logs available for review? Yes \(\square \) No \(\square \)			
Describe the local agency's plan for meeting CCH/III secondary dissemination log requirements:			
Comments:			
3.00 Responsibilities of the Contractor			
3.01 The Contractor shall maintain a security program which complies with this Security Addendum.			
Requirement met: Yes (See 3.03) No			
Comments:			
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.			
Security Officer:			
Comments:			
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. (DPS expectation: The security plan will address all security requirements in the CJIS Security Policy, whether or not they are explicitly identified in the Security Addendum. For example, wireless and encryption requirements, network documentation, firewalls, etc.)			
Requirement met: Yes, Plan approved by the local criminal justice agency \(\subseteq No \subseteq \)			
Plan Summary:			

The CSA shall ensure that all NCIC hot file transactions be maintained on an automated log

2.05

engaged in the management, development, operation, and/or maintenance of criminal justice systems and facilities. Annual refresher training shall also be provided.
Requirement met: Yes, Plan approved by the local criminal justice agency \(\square \) No \(\square \)
Plan Summary:
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. (Also reference CJIS Security Policy section 5.)
Requirement met: Yes, Plan approved by the local criminal justice agency \(\square \) No \(\square \)
Plan Summary:
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. (DPS expectations: These inspections will be in partnership with the CJA, where applicable, and could include technical as well as physical security inspections.) Requirement accepted by Contractor: Yes \(\Boxed{\text{No}}\) \(\Boxed{\text{No}}\)
Comments:
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. (DPS expectation: records will be kept by CGA/CJA regarding annual review dates and activities. The scope of the review will include validation of security requirements.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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. (This means that the CJIS Security Policy requirements are included.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:

The Contractor shall provide for a Security Training Program for all Contractor personnel

3.04

4.00 Site Security

4.01 The Contractor shall dedicate and maintain control of the facilities, or areas of facilities, that support the CGA. (DPS expectation: Contractor Site security will be included in the required Security Plan.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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. (DPS expectation: terminal security and criminal justice data security will be addressed in required Security Plan.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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.
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures. (DPS expectation: quality assurance procedures will be documented and approved by CGA/CJA.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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.
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:

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.
Requirement accepted by Contractor: Yes \Boxedom No \Boxedom
Comments:
5.05 All criminal history record information requests must be 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.
Requirement accepted by Contractor: Yes \Boxedom No \Boxedom
Comments:
5.06 The Contractor will ensure that its inquiries of CJIS Systems and any subsequent dissemination conforms with applicable FBI/CJIS policies and regulations, as set forth in (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. All disseminations will be considered as "Unclassified, For Official Use Only."
Requirement accepted by Contractor: Yes \Boxedom No \Boxedom
Comments:
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.
Requirement accepted by Contractor: Yes \Boxedom No \Boxedom
Comments:
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.
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:

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. (DPS expectation: the record checks must be completed prior to the person receiving access.)			
Requirement	accepted by Contractor: Yes \[\] No \[\]		
Comments: _			
instances whe	n a request is received by the CSA before system access is granted: (DPS expectation: In ere the CGA is a non-criminal justice agency, the criminal justice agency will perform the duties ow for the CGA.)		
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 of 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. The CGA may request the CSO to review an adverse employment decision in extenuating circumstances.		
Requirement (accepted by Contractor: Yes No		
Comments: _			

The investigation of the applicant's background shall also include contacting of employers (past or present) and personal references. (DPS expectations: the vendor and CGA will agree on the process and the screening based upon previous employers and personal references, unless it involves the discovery of criminal activity, at which point the screening will be as described in this document.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
The Security Officer shall maintain a list of personnel who successfully completed the background investigation. (DPS expectation: The approved list will be available for review by CGA/CJA and CSA. Upon termination of employment or access, the person's system access will be deleted at the contractor site and criminal justice agency customers notified so that any local system access will be likewise revoked/deleted.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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.
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:
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.
Requirement accepted by Contractor: Yes \Boxedom No \Boxedom
Comments:
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. (DPS notation: Sensitive areas include anywhere within data center housing equipment that processes CGA/CJA's data.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:

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. (DPS expectations: The systems will be dedicated to the functions of the contract, but are not restricted to providing service only to the CGA. This is a shared responsibility of the CJA/CGA/Contractor.)						
Requiremen	at accepted by Contractor: Yes \Boxedom No \Boxedom at accepted by CJA: Yes \Boxedom No \Boxedom at accepted by CGA: Yes \Boxedom No \Boxedom					
Comments:						
technical se	e system shall include the following technical security measures: (DPS expectation: These excurity measures will be documented in the required Security Plan and are a shared responsibility CGA/Contractor. See CJIS Security Policy for minimum requirements.)					
a.	a. unique identification and authentication for all interactive sessions;					
b.	b. if warranted by the nature of the contract, advanced authentication techniques in the form 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).						
Requiremen	at accepted by Contractor and the full plan is available for review: At accepted by CJA and the full plan is available for review: At accepted by CGA and the full plan is available for review: Yes No No					
Contractor	Plan summary:					
CJA/CGA F	Plan summary:					

7.03 Data encryption shall be required throughout the network passing through a shared public carrier network. (DPS expectation: Data encryption process will be documented in the required Security Plan and meet all requirements of the CJIS Security Policy. A "public network" segment for CJIS purposes is defined as a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by a criminal justice agency, i.e., a telecommunications infrastructure which supports a variety of users other than criminal justice or law enforcement. Examples of public networks/segments include, but are not limited to: dial-up and internet connections, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Description of encryption:
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. (DPS expectation: Secure storage and disposal will be documented in the required Security Plan and meet all requirements of the CJIS Security Policy.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Description of storage and disposal:
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. Sanitization 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. (DPS expectation: Sanitizing media will be documented in the required Security Plan.)
Requirement accepted by Contractor: Yes \[\] No \[\]
Description of process for sanitizing media:
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.
Requirement accepted by Contractor: Yes \[\] No \[\]
Comments:

8.02 The CGA must report security violations to the CSO and the Director, FBI, along with indications of actions taken by the CGA and Contractor. (DPS expectations: notice to the CSO will be

·	rded to the FBI CJIS Division, and constitutes notice to the Director, FBI. We will check with FBI and le an address for the FBI Director or his designee, if desired by FBI.)
Requir	rement accepted by Contractor: Yes \Boxedom No \Boxedom
Comm	ents:
8.03	Security violations can justify termination of the appended agreement.
Requir	rement accepted by Contractor: Yes \Boxedom No \Boxedom
Comm	ents:
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 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 criminal history record information must be deleted or returned to the CGA.
Requir	rement accepted by Contractor: Yes \Boxedom No \Boxedom
Comm	ents:
	The FBI reserves the right to audit the Contractor's operations and procedures at scheduled or eduled times. The FBI is authorized to perform a final audit of the Contractor's systems after ation of the Security Addendum.
Requir	rement accepted by Contractor: Yes \Boxedom No \Boxedom
Comm	ents:
9.00	Miscellaneous provisions
9.01 any pe	This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on crosns other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
Requir	rement accepted by Contractor: Yes \Boxedom No \Boxedom
Comm	ents:
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 CJIS Security Policy; and

The parties are also subject to applicable federal and state laws and regulations. **Requirement accepted by Contractor: Yes | No | Comments: _____ 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. **Requirement accepted by Contractor: Yes | No | Comments: _____ 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. **Requirement accepted by Contractor: Yes | No | **Comments: _____ 9.05 All notices and correspondence shall be forwarded by First Class mail to:

(4) Title 28, Code of Federal Regulations, Part 20.

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; (2) the NCIC 2000 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 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
Printed or Typed Contractor Employe	ee Name		
	D.O.D.		
Sex: Race:	DOB:	State/ID or DL:	
Signature of Contractor Representative	ve		Date
Printed or Typed Name of Contractor	Representative		
		_	
Organization and Representative's Ti	tle		

Texas Signatory Page

The undersigned parties agree that the attached <i>CJIS Security Addendum</i> and () responses to the requirements of that addendum are now a part of the contract between the () and () for (). The parties agree to abide by all requirements of the <i>CJIS Security Addendum</i> , and it shall remain in force for the term of the contract. Any violation of this addendum constitutes a breach of the contract. To the extent there is a conflict between a confidentiality clause in the underlying contract and the CJIS Security Addendum and/or the CJIS Security Policy, the CJIS Security Addendum and the CJIS Security Policy shall govern any information covered by the CJIS Security Addendum and/or the CJIS Security Policy.	
Printed Name of Agency Representative	
Signature of Agency Representative	Title
Agency Name and ORI	Date
Printed Name of Vendor (Contractor) Representative	
Signature of Vendor (Contractor) Representative	Title
Vendor Organization Name	Date