Florida Department of Law Enforcement (FDLE)
INFORMATION SYSTEMS SECURITY ADDENDUM

The purpose of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, agency policies and standards.

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 FDLE's information resources are not compromised. Security measures 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 Contractor personnel assigned to FDLE.

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 member of FDLE, who manages the agreement between the Contractor and agency.

1.03 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.

1.04 Contractor Security Officer (CSO) – an individual designated by the Contractor to administer the Contractor's security program as it pertains to this contract.

1.05 Information Security Manager (ISM) – a member of FDLE, designated by the agency head, to administer FDLE's information security program.

2.00 Responsibilities of FDLE

2.01 FDLE will appoint an AC.

2.02 The AC has the following responsibilities:

a. Understand the communications and records capabilities and needs of the Contractor which is accessing federal and state records through or because of its relationship with FDLE;

b. Participate in related meetings and provide input and comments for system improvement;

c. Receive information 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 the Florida Crime Information Center (FCIC) System, schedule the operators for testing or a certification exam. 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 FDLE information systems;

h. Where appropriate, ensure compliance by the Contractor with Criminal Justice Information System (CJIS) security requirements; and

i. Ensure that Contractor staff undergo background investigations prior to accessing FDLE information systems.

3.00 Responsibilities of the Contractor

3.01 The Contractor shall maintain a security program which meets the requirements of this Security Addendum.

3.02 The Contractor shall assign a Contractor Security Officer (CSO) accountable for the management of this security program. This person shall coordinate with the AC and ISM to establish the Contractor's security program. The Contractor Security Officer for this contract is Christopher Sheppard.

3.03 The Contractor shall ensure that all Contractor personnel assigned to FDLE read this Security Addendum and sign the Certification form attached to this addendum. Signed Certification forms shall be delivered to FDLE's Information Security Manager.

3.04 The Contractor shall establish and maintain 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 FDLE information systems or records located therein must be communicated to the AC immediately.

3.05 The Contractor's facilities will be subject to unannounced security inspections performed by FDLE. These facilities are also subject to periodic audits.

3.06 The security plan is subject to annual review by the AC and the Contractor. During this review, efforts will be made to update the program in response to security violations, changes in policies and standards, and/or changes in federal and state law and technology.

3.07 The Contractor and its employees will comply with all federal and state laws, rules, procedures and policies formally adopted by FDLE, Florida's Agency for Enterprise Information Technology, and Federal Bureau of Investigations.

4.00 Site Security

4.01 The Contractor shall dedicate and maintain control of the facilities, or areas of facilities, that support FDLE, when applicable.

4.02 All personal computers and/or terminals physically or logically connected to the computer system accessing FDLE information systems must be segregated and screened against unauthorized use or observation.

5.00 System Integrity

5.01 Only employees of the Contractor and such other persons as may be granted authorization by the AC shall be permitted access to the system.

5.02 The Contractor shall maintain appropriate and reasonable quality assurance procedures.

5.03 Access to the system shall be available only for official purposes consistent with the appended Agreement. Any dissemination of FDLE data to authorized employees of the Contractor is to be for their official purposes.

5.04 Information contained in or about the system will not be provided to another entity without prior written authorization by the AC.

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.

5.06 The Contractor will ensure that its inquiries of FDLE information systems and any subsequent dissemination conform to applicable laws, rules, and policies, as set forth in:

(1) Chapter 817, F.S. Fraudulent Practices
(2) Chapter 119, F.S. Public Records
(3) Chapter 943, F.S. Law Enforcement Act
(4) and this Security Addendum;

5.07 The Contractor shall protect against any unauthorized persons gaining access to the equipment, any of the data, or the operational documentation for the criminal justice information system. In no event shall copies of messages or criminal history record information be disseminated other than as envisioned and governed by the appended Agreement.

6.00 Personnel Security

6.01 A background investigation will be conducted on all Contractor employees and the Contractor's vendors which provide system maintenance support.

6.02 The background investigation will conducted by FDLE. This investigation includes an employment check, reference check, credit check, drug screen, and submission of a completed applicant fingerprint card. State and national record checks by fingerprint identification will be conducted for all personnel who manage, operate, develop, access and maintain criminal justice information systems and facilities. Record checks must be completed prior to employment.

6.03 When identification of the applicant with a criminal history has been established by fingerprint comparison, FDLE will review the matter. A Contractor employee found to have a criminal record consisting of any felony convictions or of misdemeanor offenses which demonstrate a pattern of disregard for lawful behavior is disqualified. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

6.04 If an adverse employment determination is made, access will be denied and the Contractor's Security Officer will be notified in writing of the access denial. This applicant will not be permitted to work on the contract with the FDLE. The Contractor shall be notified of the adverse decision. The Contractor may request FDLE to review an adverse employment decision.

6.05 FDLE's Security Officer shall maintain a list of personnel who successfully completed the background investigation.

6.06 FDLE 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 FDLE and available for audit purposes.

6.07 FDLE shall ensure that each Contractor employee authorized to access CJIS network terminals or information provided there from is specially trained in the state and federal laws and rules governing the security and integrity of criminal justice information.

6.08 Visitors to sensitive areas of Contractor facilities must be escorted at all times by a Contractor employee with clearance. Names of all visitors shall be recorded in a visitor log, to include date and time of visit, name of visitor, purpose of visit, name of person visiting, and date and time of departure. The visitor logs shall be maintained for five years following the termination of the contract.

7.00 System Security

7.01 Transmission, processing, and storage of criminal justice information shall be conducted on dedicated systems. Increased reliance should be placed on technical measures to support the ability to identify and account for all activities on a system and to preserve system integrity.

7.02 The system shall include the following technical security measures:

a. unique identification and authentication for all interactive sessions;

b. if warranted by the nature of the contract, advanced authentication techniques in the form of digital signatures and certificates, biometric or encryption for remote communications;

c. security audit capability for interactive sessions and transaction based logging for message-based sessions; this audit shall be enabled at the system and application level;

d. access control mechanisms to enable access to be restricted by object (e.g., data set, volumes, files, records) to include the ability to read, write, or delete the objects;

e. ORI identification and access control restrictions for message based access;

f. system and data integrity controls;

g. access controls on communications devices;

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

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

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

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

8.00 Security Violations

8.01 Consistent with Section 3.05, the Contractor agrees to inform the AC and ISM 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 is grounds for termination, which shall be immediately reported to the AC in writing.

8.02 The ISM will be responsible for reporting security violations to Florida's Agency for Enterprise Information Technology along actions taken by FDLE and Contractor.

8.03 Security violations can justify termination of the appended agreement.

8.04 Upon notification, FDLE 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 telecommunications link to FDLE information systems.

8.05 FDLE will provide the Contractor with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to FDLE by the Contractor. Upon termination, the Contractor's records containing criminal history record information must be deleted or returned to FDLE.

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

9.00 Miscellaneous Provisions

9.01 The parties are also subject to applicable federal and state laws and regulations.

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

9.03 This Security Addendum may only be modified by amendments signed by authorized representatives of FDLE and the Contractor.

9.04 Security-related notices and correspondence shall be forwarded to:

FDLE
Information Technology Services
Attention: Information Security Officer
2331 Phillips Road
Tallahassee, FL 32308

FDLE
INFORMATION SYSTEMS SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I have read and understand the contents of the Security Addendum and the documents referenced therein and agree to be bound by their provisions.

I recognize that information obtained from FDLE information systems should be used only for its intended business purposes and that there is the potential for great harm if misused. I acknowledge that access to FDLE 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 FDLE information systems 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.

Signature	
Name	
Title	
Company Name	
Date	