

Data Security and Privacy Terms

The below Data Security and Privacy Terms (the Terms) set forth the standards and responsibilities of the Contractor to maintain the confidentiality, integrity, and availability of data when providing services to the State of Ohio (State). These Terms are in addition to the Contract terms and conditions. In the event of a conflict between the Contract and these Terms, the most stringent standard will prevail.

I. Definitions

- A. Contract** means the contract entered into between the Contractor and the State to which these Terms are attached and/or incorporated.
- B. Contract Data** means State Data to which the Contractor has access, transmits, processes, possesses, creates or stores in providing services to the State. Contract Data may include Confidential Data.
- C. Contractor** means the person or entity with whom the State has entered into the Contract and, for purposes of these Terms, includes employees, subcontractors, agents or other personnel under the authority or control of the Contractor performing the work or providing the services under this Contract.
- D. Confidential Data** means any type of data that is required to be protected by law or regulation, is intended for confidential use, or may not be copied or removed from the State's operational control without authorized permission. Confidential Data includes Personal Information as defined in Ohio Revised Code 1347.01 that is required to be protected as confidential by law or regulation. Confidential Data also includes data that, if compromised, may result in loss of life, serious injury, or other harm to an individual or group, or disruption to critical agency operations.
- E. Security Incident** means a confirmed, successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system involving Contract Data, either by Contractor personnel and/or within the Contractor's administratively controlled environment(s).
- F. State Data** means all data and information provided by, created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including Contract Data and Confidential Data.

II. Requirements

A. Information Security Program

The Contractor must maintain a reasonable information security program consisting of policies, procedures, tools, and personnel designed to maintain the confidentiality, integrity, and availability of data and of services provided to the State. The Contractor's information security program must reasonably align to the current version of one or more of the following industry-recognized cybersecurity frameworks, as applicable to the work under the Contract:

1. National Institute of Standards (NIST) Special Publication 800-53 (NIST 800-53);
2. NIST 800-171
3. NIST Cybersecurity Framework (NIST CSF);
4. International Organization for Standardization 27001 (ISO27001);
5. Center for Information Security (CIS) Critical Security Controls;
6. Health Information Trust Alliance (HiTRUST);
7. Cybersecurity Maturity Model Certification (CMMC);
8. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); and/or
9. Payment Card Industry Data Security Standard (PCI-DSS).

B. Background Investigations of Contractor Personnel

Prior to any individual doing any of the following, the Contractor must validate and confirm the identity of the individual by initiating and receiving a Federal Bureau of Investigation (FBI) national fingerprint-based background check:

1. Working onsite at a State-owned, leased, or managed location;
2. Remotely accessing an internal State information system; or
3. Accessing Confidential Data, and at the Contractor's expense.

If an FBI national fingerprint-based background check cannot be initiated (i.e., an FBI Background Check Reason Code¹ is not available), then the Contractor must initiate and receive an Ohio Bureau of Criminal Investigation fingerprint-based background check or the individual's state of residence equivalent, where permitted by law. For the duration of the Contract, the Contractor must ensure all of the following for each individual performing work under the Contract:

1. The individual is eligible to perform work in the United States;
2. The individual is physically located in the United States while performing work on the Contract unless a waiver of this requirement is received from the State pursuant to the Contract;

¹ FBI Reason Fingerprint Codes available at: [Publications for BCI and Background Checks - Ohio Attorney General Dave Yost](#)

3. The individual is not currently charged with, in a diversion program for, or convicted of any of the following:
 - a. felony;
 - b. crime of violence; or
 - c. offense involving fraud, theft, or dishonesty;
4. The individual is not designated as a Specially Designated National by the Office of Foreign Asset Control (OFAC); and
5. The individual is not suspected of working for a foreign government or criminal organization.

The State reserves the right to conduct investigations of any individual working onsite at a State owned, leased, or managed location or remotely accessing a State information system or Confidential Data. Such investigation may include fingerprinting; criminal, tax, and driving record checks; drug testing; licensing and credential checks; and/or employment history verification. Access to any of the aforementioned locations, information systems, or data may be denied at any time if, in its sole discretion, the State determines it would be in its best interests.

If any individual who intends to perform work does not initially meet or if at any point during the performance of work, does not meet, the requirements detailed in this section, the Contractor must either not permit those individuals to begin to perform the work under the Contract or must terminate the individual's performance of the work under the Contract immediately, as applicable.

C. Security Incidents

The Contractor is responsible for Security Incidents that occur during the performance of the work under the Contract, including the detection of, response to, and recovery from Security Incidents to minimize the impact to the State.

The Contractor must report to the State in writing within 48 hours of the Contractor becoming aware of a Security Incident and must reasonably cooperate with the State to mitigate the impact to the State of the Security Incident. The Contractor must work with the State at the beginning of each engagement to establish Security Incident reporting procedures. If no procedure is established, the Contractor must report Security Incidents to the State via email at CSC@ohio.gov and/or by calling 877-644-6860.

Within five business days after an initial Security Incident report to the State, the Contractor must begin providing follow-up reports of the Security Incident to the State containing pertinent information about the scope, data elements, indicators of compromise, threat actors, and remediation efforts, as available.

The Contractor must preserve sufficient evidence about the Security Incident to:

1. Ensure the Security Incident records are accurate,
2. Facilitate an investigation into the Security Incident, and

3. Determine the extent of the Security Incident.

The Contractor is responsible for all associated costs of the Security Incident, including notification to impacted individuals and applicable credit monitoring for those impacted individuals.

The Contractor must comply with all applicable laws that require the notification of individuals, or with other reasonable direction of the State for notification when Confidential Data is involved.

The State reserves the right to conduct an independent investigation of the Security Incident, and the Contractor must reasonably cooperate with the investigation. The independent investigation may be conducted by a State agency or a third-party acting on behalf of the State.

D. Privacy

The Contractor must publish a privacy policy that includes the Contractor's procedure for responding to requests to access, correct, or delete Confidential Data.

E. Generative Artificial Intelligence

The Contractor must disclose the use of generative artificial intelligence (AI) to the State when producing work that will be owned by the State or the integration of generative AI in products, services, or solutions used by the State. The Contractor will reasonably cooperate in the State's review of the generative AI solution by responding to associated requests. The Contractor must not utilize Confidential Data in training generative AI models except as specifically approved by the State.

F. Data Return or Destruction

Upon completion of the work under the Contract or upon termination or expiration of the Contract, the Contractor must promptly destroy or return to the State, in a format designated by the State, all Contract Data received from or through the State. Notwithstanding the foregoing, the Contractor may keep a copy of the Contract Data to comply with contractual, legal, or record keeping obligations, and any such retained Contract Data is subject to the requirements of this Contract for so long as the Contractor has the Contract Data in its possession.

III. Requirements for Contractor or Cloud Hosted Solutions

A. Data Hosting

All Contract Data must be hosted within the contiguous United States at a minimum of two data center facilities at two different and distant geographic locations, in high-availability configurations. The Contractor must ensure appropriate physical and

environmental controls are implemented to maintain the confidentiality, integrity, and availability of Contract Data.

B. Data Security

All Contract Data in Contractor's possession must be encrypted at rest and during transit using industry standard validated encryption methods that meet or exceed the requirements set forth by NIST Federal Information Processing Standards (FIPS) 140-2.

The Contractor may not sell, rent, lease, or disclose any Contract Data to any third party, except as permitted under the Contract or required by applicable law, regulation, or court order.

Prior to promoting or releasing source code into production, the Contractor must utilize industry best practices to scan source code for vulnerabilities and remediate vulnerabilities using a risk-informed approach at no cost to the State.

C. Independent Third-Party Audit

The Contractor must obtain, at its expense, an independent third-party audit of its security controls in place for the hosted solution, product, or service. This audit must be conducted at least biennially for the duration of the Contract, renewed as required, and be one of the following audit types:

1. Federal Risk and Authorization Management Program (FedRAMP);
2. GovRAMP;
3. Service Organization Control (SOC 2) Type II;
4. ISO 27007;
5. HiTRUST;
6. CSA STAR Level 2 or Level 3; or
7. CMMC Level 2 or Level 3.

The Contractor, at its sole expense, must address material issues and weaknesses identified in each audit as they pertain to the services provided under this Contract.

The results of the audits must be provided to the State at Compliance@das.ohio.gov within 30 days of the Contractor's receipt of its audit results. The results of the audit provided to the State are considered Confidential Information under the Contract.

When required by law, rule, or regulation, or if the Contractor fails to obtain the required audit or obtains an adverse opinion on an independent third-party audit, the State may perform an information security audit of the hosted solution at its own expense. The State will provide a 30-day written notice prior to beginning the audit and the audit will take place during the Contractor's normal business hours. Before beginning the audit, the State and Contractor will reasonably agree on the scope,

duration, and other parameters of the audit. The State reserves the right to utilize a third-party contractor to perform the audit subject to reasonable approval by the Contractor.

IV. Requirements for Specific Use Cases

**[Sections A-E below to be included only when applicable.
Remaining sections, along with this note, should be deleted if not applicable.]**

A. Contractor Access

When the Contractor accesses State network systems, data, and facilities, including remotely, the Contractor must maintain a robust security capability that incorporates generally recognized system hardening techniques. The Contractor must use appropriate measures to ensure that Contract Data is secure before transferring control of any systems or media on which Contract Data is stored. The method of securing the Contract Data must be in alignment with the required data classification. The Contractor must not permit Contract Data to be loaded onto portable computing or storage devices, such as thumb drives. The Contractor must use multifactor authentication to limit access to systems that contain Contract Data.

B. Family Educational Rights and Privacy Act

When the Contractor is handling Contract Data that includes student information, the Contractor must comply with all applicable provisions of Ohio and federal laws regarding student information, including Parts B and C of the Individuals with Disabilities Education Act (20 U.S.C. 1400 and Title 34 of the Code of Federal Regulations Part 300, and 20 U.S.C. 1400 and Title 34 of the Code of Federal Regulations Part 303, respectively) and the Family Educational Rights and Privacy Act (20 U.S.C. 1232) (FERPA) or its State equivalent including any amendments or other relevant provisions of federal law as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations. Nothing in this Contract will be construed to allow either party to maintain, use, disclose, or share student information in a manner not allowed by either state or federal laws or regulations.

C. HIPAA Compliance

When the Contractor is handling Contract Data that includes protected health information within the scope 45 C.F.R. Part 164, the security and privacy rules of Health Insurance Portability and Accountability Act (HIPAA), the Contractor must comply with the data handling and privacy requirements of HIPAA and its associated regulations. Additionally, some or all of the Contract Data may be client identifying information covered by 42 C.F.R. Part 2. Contractor may only disclose such client identifying information back to the State and is bound in all respects by the regulations of 42 C.F.R. Part 2. If required, the Contractor must execute a business associate agreement with the State when handling protected health information.

D. Federal Tax Information

When the Contractor is handling Contract Data that includes Federal Tax Information (FTI), the Contractor must comply with the IRS Publication 1075 safeguards below.

The State will conduct initial background investigations on Contractor personnel who will have access to Federal Tax Information (FTI) that must be favorably adjudicated before being permitted to access the FTI. A new background investigation may be conducted every five years thereafter for personnel who already have access to FTI.

If any Contractor personnel refuses to have a background investigation completed or has an unfavorably adjudicated background investigation completed, the State will terminate that personnel's access to the Contract Data.

All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in Internal Revenue Service (IRS) Publication 1075. The language in this section may not be modified by Contractor and any proposed language changes listed in Contractor's responses in this section will not be considered. For purposes of this section, "agency" means the applicable State entity.

1. Performance

In the performance of the contract, the contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- a. All work will be performed under the supervision of the contractor.
- b. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- c. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- d. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

- e. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- f. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- g. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- h. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- i. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- j. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.
- k. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.
- l. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the

term “subcontractor” includes any officer or employee of the subcontractor with access to or who uses FTI.

- m. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

2. IRS 1075 Criminal/Civil Sanctions

- a. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- b. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
- c. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- d. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations

established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- e. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

3. Inspection

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

E. Criminal Justice Information

When the Contractor is handling Contract Data that includes criminal justice information (CJI), the Contractor must comply with the requirements in this section.

The State will conduct initial background investigations on Contractor personnel who will have access to CJI that must be favorably adjudicated before being permitted to access the CJI. A new background investigation may be conducted every five years

thereafter for personnel who already have access to CJI and require continued access.

If any Contractor personnel refuses to have a background investigation completed or has an unfavorably adjudicated background investigation completed, the State will terminate that personnel's access to the Contract Data.

Contractor acknowledges that this Contract is subject to the requirements, conditions and restrictions set forth in the following:

- a. The National Crime Information Center (NCIC) Operating Manual (available at [Criminal Justice Information Services](#), call the help desk);
- b. The Criminal Justice Information Services (CJIS) Security Policy (available at [CJIS Security Policy Resource Center — LE](#)); and
- c. Title 28, Code of Federal Regulations, Part 20 (available at [CFR 2010 Title 28 Vol 1 Part 20 - CRIMINAL JUSTICE INFORMATION SYSTEMS](#)) as the manual, policy, and regulations may be revised, amended or replaced. Further, Contractor must require all employees, independent contractors and/or any other consultant performing work for the Contractor under this Contract to complete and submit to the State the Certification page of the Federal Bureau of Investigation, CJIS Security Addendum and Certification set forth in Appendix H of the CJIS Security Policy, the relevant portions of the current version are attached to these Terms below.

APPENDIX H 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:

Information Security Officer
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.

X

Printed Name/Signature of Contractor Employee

Date: Click or tap to enter a date.

X

Printed Name/Signature of Contractor Representative

Date: Click or tap to enter a date.

X

Organization and Title of Contractor Representative