MEMORANDUM OF UNDERSTANDING BETWEEN THE INDIANA STATE POLICE AND THE INDIANA OFFICE OF TECHNOLOGY

CONTRACT # 0000000000000000000096439

This memorandum of Understanding (this "MOU") is made between the Indiana State Police ("ISP"), a criminal justice agency, and the Indiana Office of Technology ("IOT"), a non-criminal justice agency, to ensure compliance with the FBI's Criminal Justice Information Services Policy (the "CJIS Security Policy"), which is attached hereto as Exhibit A. Additionally, the Criminal Justice Information Services Certification, which is attached hereto as Exhibit B. This MOU sets forth the Parties' rights and responsibilities with regard to IOT's administration of computer systems and network infrastructure that interface directly or indirectly with ISP's systems (which are commonly referred to as "IDACS," "AFIS," and/or "CHRIS") for the interstate and intrastate exchange of criminal justice information.[1]

RECITALS

WHEREAS, ISP is the FBI's CJIS Systems Agency for the State of Indiana.

WHEREAS, in that capacity, ISP administers and enforces the provisions of the CJIS Security Policy with regard to all criminal justice agencies at all levels of government within the State.

WHEREAS, pursuant to the CJIS Security Policy, ISP may designate a non-criminal justice agency to perform certain criminal justice functions for it.

WHEREAS, ISP has designated IOT to provide information technology support services for ISP.

WHEREAS, pursuant to the CJIS Security Policy, IOT is thus considered to possess access to criminal justice information that ISP has received from the FBI ("CJI"), regardless of any actual need, practice, or attempt to access CJI in the course of providing such services.[2]

---

[1] For the purposes of this MOU, "computer systems and network infrastructure that interface directly or indirectly with ISP's systems" means all ISP systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any ISP system or related network infrastructure, including NCIC Programs that may be subsequently designed and/or implemented within ISP for the purpose of exchanging criminal justice information.

[2] For the purposes of this MOU, "CJI" means "any information from any source where such information is originally obtained by electronic access to the Indiana Data and Communication System ("IDACS"), the Indiana Criminal History Record Information System ("CHRIS"), or the Indiana Automated Fingerprint Identification System ("AFIS"). Such sources include, but are not limited to: the FBI Interstate Identification Index ("III"), National Crime Information Center ("NCIC"), and National Instant Check System ("NICS"); the Indiana Bureau of Motor Vehicles ("BMV") Driver and Vehicle Registration System ("STARS"); and any other state Driver and Motor Vehicle Registry or other information source available via The International Justice and Public Safety Network ("Nlets").

WHEREAS, pursuant to the CJIS Security Policy, IOT must enter into an agreement with ISP which stipulates that management control of the criminal justice function – in this case the provision of information technology support services – remains solely with ISP.

AND WHEREAS, the Parties have agreed to enter into such a memorandum of understanding.

NOW, THEREFORE, the Parties hereby agree to the following terms and conditions:

AGREEMENT

A. Duties

1. In accordance with the CJIS Security Policy, the Parties agree that – with respect to computer systems and network infrastructure that interfaces directly or indirectly with the State of Indiana network for the intrastate or interstate exchange of criminal justice information – ISP shall have the ultimate authority via managed control to set, maintain, and enforce the following:

    a. Priorities.

    b. Standards for the selection and supervision of personnel who have access to CJI and for discontinuing their access.

    c. Policy governing operation of applications, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems, insofar as the applications and equipment are used to process or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

    d. Restriction of unauthorized personnel from access to or use of any applications or computer or networking equipment accessing CJI on the State of Indiana network or any network segment connected to the State of Indiana network.

    e. Compliance with all rules and regulations of the ISP, ISP Security Policies, and CJIS Security Policy with regard to the operation of all systems or network segments with access to CJI.

2. Under all circumstances, management control of the criminal justice function remains solely with ISP, and in furtherance thereof, IOT agrees to:

    a. Provide information technology support services to ISP in order to assist ISP in the administration of criminal justice.

b. Provide ISP with the names and assignments of any IOT personnel who have the ability to access any applications or computer or networking equipment that contain CJI on the State of Indiana network or any network segment connected to the State of Indiana network.

c. Submit the above-referenced IOT personnel for national, fingerprint-based background checks, the outcome of which shall by used by ISP to determine whether such personnel will be approved to have access to CJI.

d. Require IOT personnel who are approved to have access to CJI to take the ISP-provided CJIS Security Awareness Training for Information Technology Personnel within six (6) months of appointment to any position or responsibility providing access to or use of any applications or computer or networking equipment accessing CJI; and further to retake such training every year thereafter, so long as such personnel has access to or use of any applications or computer or networking equipment accessing CJI.

B. Scope and Authority

1. This MOU does not confer, grant, or authorize any rights, privileges, or obligations on any persons or entities other than the referenced Parties "IOT" and "ISP".

2. Members of IOT and ISP will abide by all aspects of the CJIS Security Policy (CJISSECPOL) when performing functions with unrestricted access to unencrypted CJI for ISP. The parties are subject to applicable federal and state laws and regulations. The ISP-provided CJIS Security Awareness Training, which is discussed above in Section A.2.d , will provide training on the substance of the applicable sections of the CJIS Security Policy; Title 28, Code of Federal Regulations, Part 20; and any other federal and state laws that may be applicable.

3. The terms set forth in this MOU 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.

C. Term and Termination

1. This MOU will begin the date of the last signature and will be effective for two (2) years**.**

2. Either party may terminate this MOU, in whole or in part, upon thirty (30) days advance written notice to the other party.

3. Either party may immediately terminate this MOU should the other party breach a material term.

4. **Termination for Convenience:** This Contract may be terminated,

in whole or in part, by the State, which shall include and is not limited to IDOA and the State Budget Agency whenever, for any reason, the State determines that such termination is in its best interest. Termination of services shall be effected by delivery to the Contractor of a Termination Notice at least thirty (30) days prior to the termination effective date, specifying the extent to which performance of services under such termination becomes effective. The Contractor shall be compensated for services properly rendered prior to the effective date of termination. The State will not be liable for services performed after the effective date of termination. The Contractor shall be compensated for services herein provided by in no case shall total payment made to the Contractor exceed the original contract price or shall any price increase be allowed on individual line items if canceled only in part prior to the original termination date. For the purposes of this paragraph, the parties stipulate and agree that IDOA shall be deemed to be a party to this Contract with authority to terminate the same for convenience when such termination is determined by the Commissioner of IDOA to be in the best interests of the State.

5. **Funding Cancellation:** As required by Financial Management Circular 3.3 and IC § 5-22-17-5, when the Director of the State Budget Agency makes a written determination that funds are not appropriated or otherwise available to support continuation of performance of this Contract, this Contract shall be canceled. A determination by the Director of State Budget Agency that funds are not appropriated or otherwise available to support continuation of performance shall be final and conclusive.

D. Agency Contacts

Contact information for the Parties is as follows:

Captain Doug Hutchinson
CJIS Systems Officer (CSO)
Indiana State Police
(812)-699-7217
DHutchinson@isp.in.gov

Hemant Jain
Chief Information Security Officer
Indiana Office of Technology
(317)-232-8376
HJain@iot.in.gov

In Witness Whereof, each Party, through their duly authorized representatives, enters into this MOU. The parties, having read and understood the foregoing terms of this MOU, do by their respective signatures dated below agree to the terms thereof.

STATE OF INDIANA

Signed by:
By: Hemant Jain - 00067
35584D5B0B2B463...

Title: CISO

Date: 6/4/2026 | 10:07 EDT

Indiana State Police

Signed by:
By: Kelly Thompson Mitchell - 100
CB858BDCC14248F...

Title: CFO, ISP

Date: 6/4/2026 | 12:37 EDT

Electronically Approved by: State Budget Agency By: (for) Chad Ranney, State Budget Director	

Exhibit A

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

Exhibit B

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative