Alabama Law Enforcement Agency

Standard Contract Addendum for Criminal Justice Information Systems (CJIS) Compliance

This Standard Contract Addendum for Criminal Justice Information Services (CJIS) Compliance ("Addendum") is entered into between the Alabama Law Enforcement Agency ("ALEA") and xxxxxxxx ("Contractor") who, by virtue of being required to sign this addendum, is subject to the Federal Bureau of Investigation (FBI) CJIS Security Policy (CSP). The parties agree that the Addendum supplements the contract between ALEA and Contractor that it is attached hereto.

Defined Terms.

The following definitions are used in this Addendum:

"CJIS Policy" means the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy that is in effect as of the effective date of the Enrollment related to this Agreement and any successor versions brought into effect by the FBI during the term of the contract, but excluding draft versions of CJIS Policy, versions of CJIS Policy released for comment or review and similar proposed policy versions that may be released by the FBI but not finally adopted.

"CJIS Security Addendum" means the CJIS Security Addendum included in Appendix H to the CJIS Policy.

"Continental United States" means the area of the United States of America comprising the 48 states that are south of Canada and north of Mexico (known as the lower 48 states) and the state of Alaska.

"Criminal Justice Information" (CJI) is defined in the CJIS Policy and is established by ALEA. For clarity, ALEA or other law enforcement data that is needed for or used in the performance of services or functions under the contract associated with this addendum will, to the extent it is stored and processed by Contractor, be treated as if such data is CJIS data for purposes of this Addendum.

"CSA" means the CJIS Systems Agency (as that term is defined in the CJIS Policy) for the State, which within the State of Alabama is the Alabama Law Enforcement Agency (ALEA).

"Key Contractor Personnel" means Contractor's Representatives who engage in the delivery of Services covered by this addendum and who have physical or logical access to unencrypted CJI.

"Security Incident" means any:

- **(a)** unlawful or unauthorized access to any ALEA data stored on Contractor's equipment or in Contractor's facilities, resulting in loss, disclosure, or alteration of ALEA or other law enforcement agency data; or
- **(b)** unlawful or unauthorized access to such facilities or equipment, resulting in loss, disclosure, or alteration of ALEA or other law enforcement agency data.

"Representative" means any one of the Contractor's employees, contractors, advisors, consultants, or Affiliates.

"State" means the State of Alabama.

1. **CJIS Security Addendum**

   Contractor will support ALEA's compliance with the CJIS Policy by executing an agreement containing the CJIS Security Addendum by reference and by delivering an executed CJIS Security Addendum to ALEA for each of its Key Contractor Personnel or Representatives as required by ALEA.

2. **Responsibilities**

   2.1

   ALEA is responsible to ensure that the CJIS Security Addendum has been signed and that each Key Contractor Personnel or Representative is approved or denied access.

   2.2

   ALEA is responsible to review services documentation to ensure that services comply with the CJIS Policy or other legal or regulatory requirements that may be applicable.

   2.3

   ALEA is responsible to determine how it can use the services in a manner compliant with the CJIS Policy, whether it can appropriately use any other services or products offered with the primary services, and to adopt and implement policies and practices for appropriate use of the services, and use (or non-use) of other services or products offered with the primary services, to achieve such compliance.

   2.4

   Contractor's use of ALEA data for provided Services. ALEA and other law enforcement agency data will be used only to provide the services under the terms of the accompanying contract, including purposes compatible with providing those services. Contractor will not use data or derive information from it for any advertising or similar commercial purposes. Contractor shall not capture, maintain, scan, index, share or use data stored or transmitted by the service, or otherwise use any data-mining technology, for any non-authorized activity.

   The services will be logically separate from any of the Contractor's consumer Online Services. Data, other data in Contractor's consumer Online Services, and data created by or resulting from Contractor's scanning, indexing, or data-mining activities of other such data, will not be commingled unless expressly approved by ALEA in advance.

2.5

Location of ALEA data at rest - Contractor will provide the services from data centers in the United States. In connection with the services, Contractor will store the data at rest in data centers only in the Continental United States.

2.6

Compliance with applicable law - Contractor will comply with all applicable laws relevant in the provision of services to ALEA and other law enforcement agencies.

2.7

Contractor's responsibility for Representatives - Contractor Representatives, including subcontractors employed by Contractor, who have access to CJI, will be within full legal jurisdiction of the United States. Contractor will ensure that all its Representatives comply with all terms and conditions set out in this section. Furthermore, Contractor accepts full liability for all acts or omissions of its Representatives as if they were Contractor's own acts or omissions.

2.8

Third party requests for ALEA data - Contractor will not voluntarily provide or grant access to ALEA data to any third party, and will not disclose ALEA data to a third party except as directed by ALEA or unless required by law.

Upon receipt of a third party request for ALEA's ALEA data:

a) Contractor will review the demand to determine if it is valid and if Contractor is required by law to disclose ALEA data. Contractor will only disclose ALEA data when required by a third party request that is issued by a third party with the authority and jurisdiction to compel Contractor to disclose the requested information and that is targeted at specific individual accounts or users associated with the Service. If Contractor is not required by law to disclose the ALEA data, Contractor will reject it;

b) Unless prohibited by law, Contractor will notify ALEA of the third party request;

c) Even where a third party request is valid and could compel Contractor to disclose the information, Contractor will use best efforts to redirect the third party to request the data from ALEA;

d) Contractor will not provide any government or related agency or entity with direct, blanket or unfettered access to ALEA data;

e) Contractor will not provide any government or related agency or entity with (a) the platform encryption keys used to secure ALEA data or (b) the ability to break such encryption;

f) Contractor will not provide any government or related agency or entity with broad, unspecific or indiscriminate access, including indirect access, to ALEA data; and

g) Contractor will not provide any government or related agency or entity with any kind of access to ALEA data if Contractor is aware that such data is used for other purposes than stated in the respective search warrant, court order, subpoena or discovery request.

In addition, Contractor will comply with ALEA's reasonable requests to respond to or oppose a third party request if it comes from a governmental entity, and will provide ALEA with the information and tools required for it to respond to such third party request, provided that such information is within Contractor's reasonable control and with such tools typically made available to other customers.

In support of the above, Contractor may provide ALEA's basic contact information to the third party. ALEA is responsible for responding to requests by a third party regarding its use of Services, such as a request to take down content under the Digital Millennium Copyright Act.

3. CJIS Policy Approach in Services

Contractor agrees to comply with all applicable requirements of the CJIS Policy, as set forth in this Addendum, including this attachment. This Attachment describes how Contractor and ALEA will fulfill their obligations under the CJIS Policy in delivery and use of the Services.

A. Considerations for Compliance with CJIS Security Policy

Contractor and ALEA have agreed certain requirements of the CJIS Policy will be fulfilled as set forth in the remainder of this section, with provisions numbered to conform to the section numbering in the CJIS Policy.

1. <u>Security Awareness Training: CJIS Policy 5.2 Policy Area 2</u>

Contractor will supplement its existing security training program as required to meet the requirements of Section 5.2 of the CJIS Policy. Required training will be delivered to Key Contractor Personnel within six (6) weeks of the later of (1) the date Contractor first enters into an Enrollment in the State (including the Enrollment amended hereby, if it is the first in the State) that is amended to contain the terms contained herein, or (2) the date ALEA notifies Contractor that Key Contractor Personnel have met the adjudication standards. Contractor will refresh training for Key Contractor Personnel on at least a biennial basis thereafter.

Contractor will maintain training records, which will be available to ALEA upon written request.

2. **Incident Response: CJIS Policy 5.3 Policy Area 3**

(a) If Contractor becomes aware of a "Security Incident," Contractor will promptly: (i) notify ALEA of the Security Incident; (ii) investigate the Security Incident and provide ALEA with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(b) Notification(s) of Security Incidents will be delivered to ALEA by phone as indicated below:

Alabama Criminal Justice Information Center Watch Desk

(334) 517-2400

In the event Contractor reasonably anticipates that a Security Incident may require legal action against involved individual(s), or where the Security Incident involves either civil or criminal action, Contractor will conduct its investigative activities under guidance of legal staff and in accordance with applicable rules of evidence to the extent consistent with the primary incident response objectives of containing, resolving, and mitigating the impact of a Security Incident to ALEA.

2. Formal Audits: CJIS Policy 5.11 Policy Area 11

(a) Audits by FBI CJIS Division. In the event the FBI CJIS Division desires to perform an audit of the Services, Contractor will cooperate with such audit in good faith. The FBI may be permitted to access ALEA's data in scope for the audit. If the FBI identifies what it believes to be deficiencies in the Services as a result of an audit, Contractor is committed to working in good faith to resolve the FBI's concerns through discussion and interaction between Contractor, ALEA, and the FBI.

(b) Audits by ALEA. In the event that ALEA desires to audit the Services pursuant to the CJIS Policy, Contractor will cooperate with such audit in good faith.

ALEA will be provided, upon request, access to detailed audit materials generated by Contractor's regular monitoring of security, privacy, and operational controls in place to afford ALEA an ongoing view into effectiveness of such controls, and ALEA may communicate with Contractor operational subject matter experts regarding the content of such

information. In the event ALEA reasonably determines this information is not sufficient for ALEA's audit objectives, then, upon the ALEA's written request, Contractor will provide ALEA or its qualified third party auditor the opportunity to communicate with Contractor's auditor and, if required, a direct right to examine the Services, including examination on premises. ALEA or its auditor may only access data belonging to ALEA or other entities in the State that have purchased or used the Services and rely on ALEA for purposes of audit.

(c) Confidentiality of Audit Materials. Audit information provided by Contractor to the FBI CJIS Division or ALEA in connection with audit activities will consist of highly confidential proprietary or trade secret information of Contractor. Contractor may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret prior to providing such information to ALEA, and ALEA will ensure Contractor's audit materials, or report(s) created by ALEA based on an audit of the Services, are afforded the highest level of confidentiality available under applicable law.

4. **Personnel Security: CJIS Policy 5.12 Policy Area 12**

(a) ALEA performs personnel screening (i.e., background checks) for Key Contractor Personnel pursuant to Section 5.12 of the CJIS Policy. ALEA is responsible to confirm that such personnel screening as ALEA determines is required has been completed prior to initial processing of CJI in the Services.

(i) To facilitate personnel screening, Contractor will deliver to ALEA the relevant information regarding Key Contractor Personnel.

5. **Cloud Computing: CJIS Policy Section 5.10 Policy Area 5.10.1.5**

Contractor must ensure compliance if using cloud computing as part of its services provided to ALEA.

B. NCIC 2000 Operating Manual

ALEA acknowledges and affirms that the NCIC 2000 Operating Manual consists of guidance and/or requirements for ALEA's use of the Services. In the event ALEA determines the NCIC 2000 Operating Manual (or any subsequent version) imposes obligations with respect to the Services that can, in ALEA's opinion, only be satisfied via changes in the manner in which the Services are operated or delivered to ALEA, ALEA may provide Contractor with written notification of the specific changes it believes to be required of Contractor in order to enable ALEA's compliance with the NCIC 2000

Operating Manual (or any subsequent version), and Contractor agrees to consider any such request(s) relayed to Contractor in good faith.

C. Termination

Should ALEA determine that Contractor is in material breach and if such breach is either incurable or not cured within 30 days following the determination of such breach, then Contractor will allow ALEA to terminate its orders for Services. For up to 90 days following such termination, ALEA may extract its ALEA data from the Services, subject to the other terms and conditions of the Agreement and Enrollment amended hereby.