State of Oklahoma

Office of Management and Enterprise Services

ADDENDUM 1 TO STATE OF OKLAHOMA CONTRACT WITH IDEMIA IDENTIFY & SECURITY USA LLC RESULTING FROM SOLICITATION NO. 0900000300

This Addendum 1 ("Addendum") is an Amendment to the Contract awarded to Idemia Identity & Security USA LLC (Idemia) in connection with Solicitation No. 0900000300 ("Solicitation") and is effective July 27, 2018.

Recitals

Whereas, the State issued a Solicitation for proposals to provide electronic fingerprinting (Livescan) for selected applicants, as more particularly described in the Solicitation; and

Whereas, the State and Idemia have negotiated the final terms under which Idemia will perform the Services under the Contract.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. **Addendum Purpose.**

   This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Idemia as of even date with execution of this Addendum. The parties agree that Supplier has not yet begun performance of work contemplated by the Solicitation.

2. **Negotiated Documents of the Contract**.

   2.1. The parties have negotiated certain terms of the Contract as follows:

   i. revisions to the document initially proposed by Idemia as contained in Attachment A to this Addendum titled "Order Form"; and
   ii. hosting terms as contained in Attachment B to this Addendum, titled, "Hosting Agreement".

2.2. Accordingly, any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

State of Oklahoma

By: _____

Name: James L. Reese, II

Title: Chief Information Officer

Date: 8/14/18

Idemia Identity & Security USA LLC

By: _____

Name: Zara Roberts Gerald

Title: SVP and General Counsel

Date: 8/9/2018

Attachment A to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH IDEMIA IDENTITY & SECURITY USA LLC
RESULTING FROM SOLICITATION NO. 0900000300

The Order Form is hereby amended as set forth below and supersedes all prior documents submitted by Idemia or discussed by the parties. The parties agree to use this Order Form or a document substantially similar in the form of this Order Form**.**

Order Form

This Order Form, effective as of the date of last signature hereto ("Effective Date"), is by and between _____, with offices at _____ ("Customer"), and Idemia Identity & Security USA LLC, with offices at 296 Concord Road, Suite 300, Billerica, MA 01821 ("Idemia" or "IDEMIA") and is a Contract Document in connection with the State of Oklahoma Contract with Idemia resulting from Solicitation No. 0900000300. (the "Contract"). Customer is any State Entity or Affiliate as defined in the Contract.

WHEREAS, under the Contract, Idemia will provide fingerprinting and related services ("Services") to Oklahoma state agencies and affiliated entities so that such agencies and affiliated entities may utilize the electronic fingerprinting (Livescan) process available through the Oklahoma State Bureau of Investigation to conduct state and national criminal history record checks for selected applicants ; and

WHERAS, the parties hereto desire to enter into an agreement under which Idemia provides Services for Customer; and

NOW THEREFORE, in consideration of the mutual covenants set forth herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Terms. The parties hereby agree that Idemia will provide the services identified in the Statement of Work attached hereto as Exhibit A ("Statement of Work" or "SOW") under the terms of the Contract..

2. Counterparts. This Order Form may be executed in several counterparts, each of which when executed and delivered shall constitute an original and all of which, when taken together, shall constitute one and the same Order Form. The signature of either of the parties may be evidenced by a facsimile or electronic (e.g., pdf) copy of this Order Form, bearing such signature and transmitted to the other party. Such signature shall be valid and binding as if an original executed copy of this Order Form has been delivered.

IN WITNESS WHEREOF, the parties cause this Order Form to be executed by their duly authorized representatives.

Idemia Identity & Security USA, LLC	_____ **("Customer")**
By:_____	By:_____
Typed Name: _____	Typed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A
Statement of Work

IDEMIA will collect the following fees from applicants and may retain all such fees.

Table 1

Item	Applicant Fees
Standard OSBI/FBI fee:	$41.00
Volunteer OSBI/FBI fee:	$28.75
CUSTOMER fee:	$XX.XX*
IDEMIA service fee	$9.25

TBD by applicable Oklahoma state agency

Optional Service Pricing – Check all that apply

☐ ***Out-of-State Fingerprinting***

Electronic fingerprinting services for out-of-state Applicants. Idemia will invoice the Customer for all fees for such services, including a local fingerprint capture fee (in addition to the standard Oklahoma fee*.
Fee per Transaction: *$39.95 local fingerprint capture fee, in addition to the standard State of Oklahoma fees identified in Table 1 of this Exhibit A.*

**Service may be optionally configured to require Applicant payment of local capture fee at or before the time of fingerprinting.*

☐ ***On-Site Mobile Fingerprinting***

Service for customers who desire on-site mobile fingerprinting anywhere in the state, within 30 business days of request, for groups of 30 or more applicants. On-site services provide added convenience and coverage for specific opportunities such as orientation sessions, new teacher hiring times or other group situations.
Fee per Transaction: *$10.00 per Applicant, in addition to the standard State of Oklahoma fees identified in Table 1 of this Exhibit A.*

UEP Premium Items

In addition to UEP core functionality, IDEMIA offers the following optional capabilities to the Oklahoma Agencies and affiliated entities:

☐ ***Admin Web Portal*** - IDEMIA's UEP software has the capability to store images of biometrics captured (photos, fingerprints, identity documents). Agencies and affiliated entities can optionally utilize Idemia's Admin Web Portal to access these biometrics for research and forensics purposes.

- ***Ticketing Tool*** – Users can manage Applicant support inquiries across multiple teams.

- ***Service Code Lookup*** – Applicants can perform a look-up by ORI or IDEMIA can identify state-specific Applicant populations to choose from.

- ***Address Verification*** - This feature validates that the street address, city, state, and zip code provided by an Applicant is a valid combination recognized by the United States Postal Service.

UEP Premium Fee, per Transaction: *$1.00 per Applicant, in addition to standard State of Oklahoma fees identified in Table 1 of this Exhibit A.*

Back-up Print Capture for Poor Quality Prints

When digitally collecting fingerprints, IDEMIA's workstation software will automatically compute quality scores for each finger. If the score for a fingerprint is below an acceptable threshold, the software will direct the Enrollment Agent to re-collect the fingerprint. If the Enrollment Agent is unable to collect a fingerprint that meets acceptable quality standards, the software will direct the Enrollment Agent to collect two sets of fingerprints. IDEMIA will always submit the best fingerprint record. However, if that print is rejected by the FBI or the OSBI's AFIS, IDEMIA will automatically submit the second-best print without requiring the applicant to revisit an Enrollment Center.
Fee per Transaction: *$1.00 per Applicant in addition to standard State of Oklahoma fees identified in Table 1 of this Exhibit A.*

Custom Engineering Requests

IDEMIA has proposed the technology needed to meet all the requirements of the State's Solicitation # 0900000300. Oklahoma state agencies and affiliated entities may request enhancements or changes to the UEP system. Based on availability of resources and other factors, IDEMIA may make such requested changes and bill the customer on a Time and Materials basis at a rate of *$175.00 per man/hour*

Agency Owned Livescan Systems

Purchase price per Live Scan Workstation: *$16,616.00*
Annual Maintenance Fees (Year 2 and after): *$1,307.00 per year*
Terms and condition of purchase, maintenance and use of such system in conjunction with Idemia's network would be set forth in a separate agreement.

Attachment B to
Addendum 1 to
STATE OF OKLAHOMA CONTRACT WITH IDEMIA IDENTIFY & SECURITY USA LLC
RESULTING FROM SOLICITATION NO. 0900000300

The Contract is hereby amended as set forth below and supersedes all prior documents submitted by Idemia or discussed by the parties. The Hosting Agreement set forth below is applicable to any State Data stored or hosted by Idemia in connection with the Contract. Unless otherwise indicated herein, capitalized terms used in this Hosting Agreement without definition shall have the respective meanings specified in the Contract.

I. Definitions

a. "State Data" shall mean all data supplied by or on behalf of State in connection with the Contract, excluding any confidential information of Idemia.

b. "Data Breach" shall mean the unauthorized access by an unauthorized person that results in the use, disclosure or theft of State Data or unencrypted Personal Data.

c. "Non-Public Data" shall mean State Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by State because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by State as Non-Public Data, or that a reasonable person would deem confidential.

d. "Personal Data" shall mean State Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended. For the avoidance of doubt, Personal Data does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

e. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the hosted environment used to perform the services.

II. State Data

a. State will be responsible for the accuracy and completeness of all State Data provided to Idemia by State. State shall retain exclusive ownership of all State Data. Non-Public Data and Personal Data shall be deemed to be State's confidential information. Idemia shall restrict access to State Data to their employees and contractors approved by the State with a need to know (and advise such employees or contractors of the confidentiality and non-disclosure obligations assumed herein). The State will notify Idemia of its approval or rejection of each contractor, following the Contractor's completion and submission of the State's security questionnaire.

b. Idemia shall promptly notify the State upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to State Data or State's use of the hosted environment. Idemia shall notify the State by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Idemia shall not disclose State Data in response to subpoenas, service or process, FOIA requests, and other legal requests for State Data without first notifying the State so that the State may seek a protective order or otherwise intervene in order to limit disclosure of State Data. Idemia agrees to so notify the State as soon as possible so that the State will have adequate time to seek a protective order or otherwise intervene.

c. Idemia will use commercially reasonable efforts to prevent the loss of or damage to State Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any State Data that may be lost or damaged by Idemia. Idemia will promptly notify State of any loss, damage to, or unauthorized access of State Data, including Personal Data, even if the Personal Data is encrypted. Idemia will use commercially reasonable efforts to reconstruct any State Data that has been lost or damaged by Idemia as a result of its negligence or willful misconduct. If State Data is lost or damaged for reasons other than as a result of Idemia's negligence or willful misconduct, Idemia, at the State's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any State Data lost or damaged.

III. Data Security

a. Idemia will use commercially reasonable efforts, consistent with industry standards, to provide security for the hosted environment and State Data and to protect against both unauthorized access to the hosting environment, and unauthorized communications between the hosting environment and the State's browser. Idemia shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures Idemia applies to its own personal data and non-public data of similar kind.

b. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, Idemia is responsible for encryption of Personal Data. For the avoidance of doubt, the State acknowledges that Personal Data stored in the database identified in Idemia's proposal to Solicitation 0900000300 will not be encrypted. Therefore, notwithstanding any terms in this Agreement to the contrary, Idemia shall have no obligation to encrypt any data, including Personal Data, that is stored in such database and shall have no liability for unauthorized use of or access to such data on the basis that it should have been encrypted. If the State desires that such Personal Data be encrypted, the parties will execute a separate agreement identifying the relevant specifications and fees therefor.

c. Idemia represents and warrants to the State that the hosting equipment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Idemia will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Idemia will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to State systems by Idemia, Idemia will promptly notify State of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Idemia has used to remediate the virus. Should the virus propagate to State's IT infrastructure, Idemia is responsible for costs incurred by State for State to remediate the virus.

d. Idemia shall provide its services to State and its users solely from data centers in the U.S. Storage of State Data at rest shall be located solely in data centers in the U.S. Idemia shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used in collecting Personal Data or kept only at Idemia's locations at which Personal Data is collected. Idemia shall permit its personnel and contractors to access State Data remotely only as required to fulfill Idemia's obligations under the Contract.

e. Idemia shall allow the State to audit conformance to the Contract terms. The State may perform this audit or contract with a third party at its discretion and at State's expense.

f. Idemia shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. Idemia may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

IV. Security Assessment

a. The State requires any entity or third-party vendor hosting Oklahoma State Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Idemia submitted to the review and met the State's minimum security standards at time the

Contract was executed. Failure to maintain the State's minimum security standards during the term of the contract, including renewals, constitutes a material breach.

b. To the extent Idemia requests a different sub-contractor than the third-party hosting vendor already approved by the State, the different sub-contractor is subject to the State's approval, the process for which is identified in Section II.a. of this Agreement. Idemia agrees not to migrate State's data or otherwise utilize the different third-party vendor hosting in connection with key business functions that are Idemia's obligations under the Contract until the State approves the third-party hosting vendor, subject to State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party hosting vendor does not meet the State's requirements under the State Certification and Accreditation Review, Idemia acknowledges and agrees it may not utilize the third-party hosting vendor to host State Data, until such third party meets such requirements.

V. Security Incident or Data Breach Notification: Idemia shall inform State of any Security Incident or Data Breach

a. Idemia may communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract or Idemia's other contractual or legal obligations. If a Security Incident involves State Data, Idemia will coordinate with State prior to any such communication.

b. Idemia shall report a Security Incident to the State identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period if required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).

c. Idemia shall: (i) maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to State at State's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Idemia; and (iv) document all Security Incidents and their outcomes.

d. If Idemia has reasonable belief or actual knowledge of a Data Breach, Idemia shall (1) promptly notify the appropriate State identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

VI. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Idemia.

a. Idemia, unless stipulated otherwise, shall promptly notify the State identified contact within 2 hours or sooner, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a Data Breach. Idemia shall (1) cooperate with State as reasonably requested by State to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services under the Contract, if necessary.

b. Unless otherwise stipulated, if a Data Breach is a direct result of Idemia's breach of its obligation to encrypt Personal data and Non-Public Data or otherwise prevent its release, Idemia shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals if required by state law – all such costs for which Idemia is liable under this Section VI.b. shall not exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) complete all corrective actions as reasonably determined by Idemia based on root cause.

c. If a Data Breach is a direct result of Idemia's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Idemia shall indemnify and hold harmless the State against all penalties assessed to the State by governmental authorities in connection with the Data Breach.

VII. **Notice:** Contact information for State for notifications pursuant this Hosting Agreement are consistent with the Contract with a copy sent to:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

And

Chief Information Security Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

And

OMES Information Services General Counsel
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

VIII. Idemia Representations and Warranties: Idemia represents and warrants the following

a. Idemia will protect State's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that it uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

b. The execution, delivery and performance of the Contract, the Hosting Agreement and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Idemia will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Idemia and any third parties retained or utilized by Idemia to provide goods or services for the benefit of the State.

c. Idemia shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting Environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

IX. Indemnity

Idemia's Duty of Indemnification. Idemia agrees to indemnify and shall hold the State of Oklahoma and State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees) (collectively "Damages") (other than Damages that are the fault of State) arising from or in connection with Idemia's breach of its express representations and warranties in this Hosting Agreement and the Contract. The State of Oklahoma and/or State shall promptly notify Idemia of any third party claims and to the extent authorized by the Attorney General of the State, allow Idemia to control the defense and any related settlement negotiations. If the Attorney General of the State of Oklahoma does not authorize sole control of the defense and settlement negotiations to Idemia, Idemia shall be granted authorization to equally participate in any proceeding related to this section but Idemia shall remain responsible to indemnify State and the State of Oklahoma for all associated costs, damages and fees incurred by or assessed to the State of Oklahoma and/or State.

X. Termination and Suspension of Service:

a. In the event of a termination of the Contract, Idemia shall implement an orderly return of State Data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of State Data.

b. During any period of service suspension, Idemia shall not take any action to intentionally erase any State Data.

c. In the event of termination of any services or the Contract in its entirety, Idemia shall not take any action to intentionally erase any State Data, other than at the State's direction, for a period of:

   i. 10 days after the effective date of termination, if the termination is in accordance with the Contract period

   ii. 30 days after the effective date of termination, if the termination is for convenience

   iii. 60 days after the effective date of termination, if the termination is for cause

   After such period, Idemia shall have no obligation to maintain or provide any State Data and shall thereafter, unless legally prohibited or otherwise stipulated, delete all State Data in its systems or otherwise in its possession or under its control.

d. The State shall be entitled to any post termination assistance generally made available with respect to the services.

e. Idemia shall securely dispose of all requested State Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the State. State Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to State upon request.

f. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR REVENUE; LOSS, INACCURACY, OR CORRUPTION OF DATA OR LOSS OR INTERRUPTION OF USE) ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE SERVICES PROVIDED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. PROVIDED, HOWEVER, THAT THE FOREGOING PROVISION SHALL NOT APPLY OR LIMIT DAMAGES, EXPENSES, COSTS, ACTIONS, CLAIMS AND LIABILITIES ARISING FROM OR RELATED TO PROPERTY DAMAGE, BODILY INJURY OR DEATH CAUSED BY EITHER PARTY; THE INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS CONTRACT, THE CONFIDENTIALITY OBLIGATIONS SET FORTH IN THIS CONTRACT; DATA SECURITY AND BREACH NOTIFICATION OBLIGATIONS SET FORTH IN THE CONTRACT; THE BAD FAITH, GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT OF EITHER PARTY OR ITS EMPLOYEES, AGENTS

AND SUBCONTRACTS; OR OTHER ACTS FOR WHICH APPLICABLE LAW DOES NOT ALLOW EXEMPTION FROM LIABILITY.