REVISED

AGENDA # _____, October 6, 2020

ALAMEDA COUNTY PROBATION DEPARTMENT

P.O. Box 2059
1111 Jackson Street
Oakland, CA 94604-2059

WENDY STILL, MAS
Chief Probation Officer

September 22, 2020

Honorable Board of Supervisors
County of Alameda
1221 Oak Street, Suite 536
Oakland, California 94612-4305

SUBJECT: APPROVE A FIRST AMENDMENT WITH IDEAS42 FOR A DATA SHARING AGREEMENT TO FACILITATE GRANT-FUNDED REENTRY SUPPORT SERVICES; PROCUREMENT CONTRACT NO. 19989

Dear Board Members:

RECOMMENDATIONS:

A. Approve a First Amendment (Procurement Contract No. 19989) with ideas42 (Principal: Josh Wright; Location: New York, New York) to add a Data Sharing Agreement to the contract to implement a web-based application to support individuals under supervision, with no change in the current term of 5/1/20 – 9/30/21, and contract amount of $151,847; and

B. Delegate authority to the Chief Probation Officer, or designee, to negotiate and execute the First Amendment and Data Sharing Agreement, subject to review and approval as to form by County Counsel and return an executed copy to the Clerk of the Board for filing.

DISCUSSION/SUMMARY:

On May 12, 2020, your Board approved (Item No. 52) a contract with ideas42, to fulfill requirements of Redesigning the Pathways Home: Alameda County's Pilot to Positive Re-entry, a grant program funded by the Bureau of Justice Assistance Innovations in Reentry Initiative (Federal Grant Award #: 2018-CA-BX-0023), to customize and implement a web-based mobile application to support individuals under supervision develop and follow incentivized plan that increase the likelihood that they will successfully complete the terms of their probation and reduce recidivism.

The Alameda County Probation Department's (ACPD) partnership with ideas42 will result in the development and implementation of a web-based mobile application, Vergil, that will allow clients on probation to identify and track steps involved in achieving their case plan goals. Data used in this application includes the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code § 13202. This shared data is highly sensitive and must be protected by all parties. The Data Sharing Agreement is the tool that addresses how and when the data will be used and the protocols for storage and destruction of data.

SELECTION CRITERIA/PROCESS:

ACPD selected ideas42 because of their extensive experience developing and implementing innovative and effective reentry support services. They are a qualified nonprofit organization that looks for deeper insights into human behavior in an incredibly unique way—into why people do what they do—and using that knowledge in ways that help improve lives, build better systems, and drive social change. Working globally, ideas42 seeks to reinvent the practices of institutions, and create better products and policies that can be scaled for maximum impact. They also teach others, ultimately striving to generate lasting social impact and create a future where the universal application of behavioral science powers a world with optimal health, equitable wealth, and environments and systems that are sustainable and just for all. For more than a decade, ideas42 has been at the forefront of applying behavioral science in the real world; and as they have developed their expertise, they have helped to define an entire field. Their efforts have so far extended to 40 countries as they have partnered with governments, foundations, non-governmental organizations, private enterprises, and a wide array of public institutions. ACPD reviewed numerous mobile applications from various vendors and ideas42 provides the most well-developed and comprehensive product on the market ready for deployment for this unique target population.

GSA approved Sole Source No. 6530 and issued a Finding Memo of Non-Competition on 4/8/2020 for ideas42. The Auditor's Office of Contract Compliance & Reporting approved Federal Small Local Emerging Business Waiver #F1572 for this contract.

FINANCING:

There is no cost associated with this amendment. Therefore, there is no impact in net County cost as a result of approving the above recommendations.

VISION 2026 GOAL:

The Pathways Home Pilot meets the 10X goal pathway of a **Crime Free County** in support of our shared visions of a **Thriving and Resilient Population** and **Safe and Livable Communities**.

Respectfully submitted,

Wendy

Wendy Still, MAS
Chief Probation Officer

Ws:mt

FIRST AMENDMENT TO AGREEMENT

This First Amendment to Agreement ("First Amendment") is made by the County of Alameda ("County") and Behavioral Ideas Lab, Inc. dba ideas42 ("Contractor") with respect to that certain agreement entered by them on June 18, 2020 (referred to herein as Procurement Contract No. 19989 or "Agreement") pursuant to which Contractor provides Reentry App Services to County.

County and Contractor, for valuable consideration, the receipt and sufficiency of which are hereby acknowledged, agree as follows:

1. Except as otherwise stated in this First Amendment, the terms and provisions of this Amendment will be effective as of the date this First Amendment is executed by the County.

2. The attached Exhibit F, Data Sharing Agreement, is incorporated into this Agreement by this reference.

3. Except as expressly modified by this First Amendment, all of the terms and conditions of the Agreement are and remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this First Amendment.

COUNTY OF ALAMEDA

By: ________________________________
Signature

Name: ____Wendy S. Still, MAS________
(Printed)

Title: ______Chief Probation Officer______

Date: ______________________________

Approved as to Form:
Donna R. Ziegler, County Counsel

By: ________________________________
K. Joon Oh, Deputy County Counsel

BEHAVIORAL IDEAS LAB, INC.
DBA IDEAS42

By: ____________________________
Signature

Name: _________________________
(Printed)

Title: __________________________

Date: __________________________

By signing above, signatory warrants and represents that he/she executed this First Amendment in his/her authorized capacity and that by his/her signature on this First Amendment, he/she or the entity upon behalf of which he/she acted, executed this First Amendment

Exhibit F

Data Sharing Agreement

This Data Sharing Agreement is incorporated into the Standard Service Agreement dated June 18, 2020, Procurement Contract No. 19989, by and between the County of Alameda, acting by and through its Probation Department (Probation) and Behavioral Ideas Lab, Inc. ("Contractor" or "ideas42") for Reentry App Services.

1. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement is to outline the terms and conditions agreed to by Contractor and Probation regarding the transfer and analysis of criminal offender record information pursuant to the authority granted in California Penal Code § 13202.

2. DEFINITIONS

"DSA" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption is required during transit and rest.

"Data Storage" refers to the state data is in when at rest. Data shall be stored on secured environments.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

"Criminal Offender Record Information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release and/or any California Law Enforcement Telecommunications Systems (CLETS) derived information. (California Penal Code §§ 11075, 13102)

3. DESCRIPTION OF DATA TO BE SHARED

Probation may share state and local Criminal Offender Record Information (CORI) related to individuals who are part of the County's realigned population. The realigned population includes clients, previously under the jurisdiction of the state, released from state prison or county to the jurisdiction of county probation. If CORI related information is shared, Contractor will be required to comply with Department of Justice (DOJ) security requirements prior to access. At the date that this DSA is signed by Probation, the data that has been identified to share with Contractor does not originate from a DOJ source.

4. DATA TRANSMISSON

a. Transmittal Method:

☒ FTP
☐ CD
☐ E-mail
☐ Hardcopy
☐ Removable Media (flash Drive)
☐ Other (please describe) ______________________
☐ Tape
☐ Database View

b. Transmittal Frequency:

☐ Weekly
☐ Annually
☒ Other Daily__________
☐ Monthly
☐ As Needed/On request
☐ Data will not be transmitted, users will access data.
☐ Quarterly
☐ One-time

c. Transmittal security: All HIPAA protected data will be encrypted prior to email transmission.

5. DATA SECURITY

All data provided by Probation shall be stored by Contractor on a secure environment with access limited to the least number of staff needed to complete the purpose of this DSA.

a. Protection of Data

Contractor agrees to store data on one or more of the following media and protect the data as described:

1) Workstation Hard disk drives. Access to data stored on local workstation hard disks will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password. If the workstation is located in an unsecured physical location the hard drive will be encrypted to protect Probation data in the event the device is stolen. Any DOJ data will be stored on a hard drive the hard drive must be destroyed before the computer is disposed of. All security updates must be current, all hot fixes and critical fixes must immediately be applied. If the computer is mobile, e.g., a laptop or tablet, the device must be managed by a mobile device management (MDM) solution that allow for a wipe and location of the device if its lost or stolen. All users with unsupervised access to CLETS data, information, and systems must have received a background clearance and be free of felony convictions, taken the DOJ training and testing, and have a signed DOJ volunteer statement and FBI addendum on file with ACPD.

2) Network server disks. Access to data stored on hard disks mounted on network servers and made available through shared folders will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password. Backup copies for disaster recovery purposes will be encrypted if recorded to removable media.

3) Optical discs (e.g., CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by Probation on optical discs will be used in local workstation optical disc drives and will not be transported out of a secure area. When not in use for the purposes authorized by the DSA, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access Probation data on optical discs will be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

4) Optical discs (e.g., CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. Access to data provided by Probation on optical discs which will be attached to network servers and which will not be transported out of a secure area will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security. Data on discs attached to such servers will be located in an area which is accessible only to authorized individuals with access controlled through use of a key, card key, combination lock, or comparable mechanism.

5) Paper documents. Any paper records will be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access. The DIN (Deutsches Institut fur Normung or German Institute for Standardization) 66399 standard for paper destruction will govern the disposal of documents when no longer needed. Such documents must be destroyed using at least a DIN Level P-4 cross-cut shredder, particle size of 4 x 40mm or .16 x1.6 in, ensuring that the documents are extremely difficult to assemble and read.

6) Data storage on portable devices or media. DOJ data should not be maintained on portable devices.

a) Probation data shall not be stored by Contractor on portable devices or media unless specifically authorized within this DSA. If so authorized, the data shall be given the following protections by Contractor:

i. Encrypt the data with a key length of at least 128 bits.

ii. Control access to devices with a unique user ID and password or stronger authentication method.

iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity if this feature is available. Maximum period of inactivity is 20 minutes.

iv. Physically protect the portable device(s) and/or media by:

- Keeping them in locked storage when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.
- Passwords must be set and be complex, they must be changed every 90 days.

b) When being transported outside of a secure area, portable devices and media with confidential Probation data will be under the physical control of Contractor staff with authorization to access the data.

c) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g., USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.

d) Portable media includes, but is not limited to; optical media (e.g., CDs, DVDs, Blu-Rays), magnetic media (e.g., floppy disks, tape, Zip or Jaz disks), or flash media (e.g., CompactFlash, SD, MMC).

b. **Safeguards Against Unauthorized Access and Re-disclosure**

Contractor shall exercise due care to protect all Criminal Offender Record Information data from unauthorized physical and electronic access. Both parties shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information provided by either party pursuant to this DSA:

1) Access to the information provided by Probation will be restricted to only those authorized staff who need it to perform their official duties in the performance of the work requiring access to the information as detailed in the Purpose of this DSA.

2) Contractor will store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

3) Unless specifically authorized in this DSA, the Contractor will not store any confidential or sensitive Probation data on portable electronic devices or media, including, but not limited to laptops, handhelds/PDAs, Ultramobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), and portable hard disks.

4) Contractor will protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

5) Contractor shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

6) Contractor shall instruct all individuals with access to the Criminal Offender Record Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this DSA, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this DSA.

7) Contractor shall take due care and take reasonable precautions to protect Probation's data from unauthorized physical and electronic access.

8) Contractor shall ensure that any material identifying individuals is not transferred, revealed, or used for other than research or statistical activities and reports or publications derived therefrom do not identify specific individuals.

c. Data Segregation

Contractor shall comply with the following requirements:

1) Probation data must be segregated or otherwise distinguishable from non-Probation data. This is to ensure that when no longer needed by Contractor, all Probation data can be identified for return or destruction. It also aids in determining whether Probation data has or may have been compromised in the event of a security breach.

2) When kept on media, Probation data will be kept on media (e.g., hard disk, optical disc, tape, etc.) which will contain no non-Probation data.

3) When stored on electronic media, Probation data will be stored in a logical container on electronic media, such as a partition or folder dedicated to Probation data.

4) When stored in a database, Probation data will be stored in a database which will contain no non-Probation data.,

5) When stored within a database Probation data will be stored within a database and will be distinguishable from non- Probation data by the value of a specific field or fields within database records.

6) When stored as physical paper documents, Probation data will be physically segregated from non-Probation data in a drawer, folder, or other container.

7) When it is not feasible or practical to segregate Probation data from non- Probation data, then both Probation data and the non-Probation data with which it is commingled must be protected as Probation data and as described in this DSA.

If Contractor or its agents detect a compromise or potential compromise in the IT security for this data such that personal information may have been accessed or disclosed without proper authorization, Contractor shall give notice to Probation within one (1) business day of discovering the compromise or potential compromise.

Contractor shall take corrective action as soon as practicable to eliminate the cause of the breach and shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed.

6. DATA OWNERSHIP

a. Probation retains ownership of all data provided pursuant to this DSA including, but not limited to, any subsets generated from the raw data, individual-level subsets derived from the raw data, and any data sets generated by addition to or in combination with other any other data.

b. Contractor may not relinquish or transfer ownership or physical custody of the data provided pursuant to this DSA to any entity.

7. DATA SHARING AGREEMENT COMPLETION/TERMINATION

a. Upon completion or termination of this Agreement or DSA, the data provided pursuant to the terms of this DSA shall be destroyed or returned to Probation with certification Contractor that the original and all copies of the data on all systems and media have been destroyed.

b. This DSA is binding as to the confidentiality, use of the data, and disposition of all data received as a result of this access, unless otherwise amended by the mutual agreement of both parties.

c. Upon execution of this Data Sharing Agreement, all Contractor staff with access to, or that have accessed the data provided pursuant to the terms of this DSA will be notified of the non-disclosure provisions of this DSA.

d. Probation may terminate, suspend, or abandon this Data Sharing Agreement with a prior written notice to Contractor as provided for in paragraph 20 of the Agreement.

8. DATA CONFIDENTIALITY

a. Regulations Governing Confidentiality of Data

i. Contractor acknowledges the confidential nature of the data received from Probation and agrees that personnel with access shall comply with all laws, regulations, and policies that apply to the protection of the confidentiality of the data. This compliance includes, but is not limited to, submitting an application as required by the CALIFORNIA DEPARTMENT OF JUSTICE, CRIMINAL JUSTICE INFORMATION SERVICES DATA ANALYSIS PROGRAM RESEARCH AND DATA REQUEST

(https://www.oag.ca.gov/sites/all/files/agweb/pdfs/corp/research-request-packet.pdf).

ii. Any willful, malicious, negligent, or knowing disclosure of the data received pursuant to this Agreement to unauthorized persons may be punishable by applicable state and federal laws, including California Penal Code §§ 11142, 13302. Any staff that unlawfully discloses confidential data that has been determined to incur any economic, bodily, or psychological harm as a result of the disclosure may also be liable for the damages incurred.

b. Limited Access to Data

i. Only staff assigned by Contractor shall have access to review, manipulate, and maintain the data received for their organization. Contractor is responsible for ensuring that only authorized staff with a business need directly related to the purpose of the Agreement and DSA will access the data received pursuant to this DSA. Signed confidentiality agreements for all staff that will have access to the data shall be obtained, maintained for the duration of the Agreement, and copies provided to Probation on request.

ii. Protected Health Information: If the dataset includes healthcare information, appropriate HIPAA safeguards shall be in place and followed by Contractor.

c. Safety and Security

Contractor acknowledges and agrees to fully comply with the necessary strict disclosure provisions that minimize directly or indirectly revealing offender level information which could jeopardize the safety or security of offenders and correctional staff, as well as the public at large.

9. CONSTRAINTS ON USES OF THE DATA RECEIVED

a. The dataset received pursuant to this DSA may be used ONLY for the purpose described in this Agreement and DSA and only for the term of the Agreement and DSA.

b. This DSA does not authorize a release of the data to any organization for discretionary use, but allows access to the data only to carry out the purposes described in this Agreement and DSA. Any ad hoc analysis or other use of the data, not expressly specified in this Agreement and DSA, is not permitted without the prior written authorization of Probation.

10. NON-DISCLOSURE OF DATA

a. Non-Disclosure of Data Requirements:

i. No person shall disclose, in whole or in part, the data provided by Probation pursuant to this Agreement to any individual or agency, unless this Agreement and DSA specifically authorizes the disclosure.

ii. Data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement and DSA and that have received approval from Probation.

iii. Staff shall not access or use the data for any commercial or personal purposes.

b. Any exceptions to these limitations must be approved in writing by Probation.

c. Penalties for Unauthorized Disclosure of Information:

Should Contractor fail to comply with any terms of this Agreement or DSA, Probation shall have the right to take such action as it deems lawfully appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties harmed or injured by unauthorized disclosure.

d. Employee Awareness of Use/Non-disclosure Requirements

Contractor shall ensure that all staff with access to the data provided pursuant to this DSA are aware of the use and disclosure requirements of this DSA and will advise all staff of the provisions of this DSA. This notification shall include all IT support staff as well as staff who will manipulate and/or analyze the data. All staff will receive Probation administered Live Scans at ACPD’s expense.

SIGNATURES

The parties have executed this Data Sharing Agreement by and through their duly authorized representatives. By signing below, signatory warrants and represents that he/she executed this Data Sharing Agreement in his/her authorized capacity and that by his/her signature on this Data Sharing Agreement, he/she or the entity upon behalf of which he/she acted, executed this Data Sharing Agreement.

Alameda County Probation Department

By: ____________________________________ Date:_________________
Wendy Still, MAS
Chief Probation Officer

Behavioral Ideas Lab, Inc. (ideas42)

By: ____________________________________ Date:_________________
Martin Laitin
Director/President

All individuals who are part of Behavioral Ideas Lab, Inc.'s (Ideas42) team and who will have access to the confidential individual-level data must sign this agreement.

Behavioral Ideas Lab, Inc. (ideas42) Staff:

By:____________________________________ Date:_________________
Alex Blau
Project Director, Vice President

By:____________________________________ Date:_________________
Sean Konz
Developer

By:____________________________________ Date:_________________
Tyler Gaw
Developer

By:____________________________________ Date:_________________
Zach Lambert
Product Lead & Implementation Specialist