Deloitte.

EXHIBIT B

Agreement Regarding Non-Disclosure of Information; Ownership of Work Product; Non-Compete ("Agreement")

You will be performing services for Deloitte Consulting LLP ("Deloitte Consulting") in connection with either an engagement for a client of Deloitte Consulting ("Client") or an internal project of Deloitte Consulting (as applicable, the "Project"). For the purposes of these terms, "Deloitte Consulting" shall mean Deloitte Consulting LLP and its subsidiaries, successors and assigns.

1. In performing these services, you will have access to proprietary and confidential information of Deloitte Consulting and/or the Client and, in order to permit Deloitte Consulting to provide you with such access, you agree that:

   (a) Any information delivered or disclosed by Deloitte Consulting, the Client, or others acting on its or their behalf, to you incidental to or in connection with performance of the services, whether such delivery or disclosure occurred before or after execution of this Agreement (collectively, the "Confidential Information"), shall be and remain the property of Deloitte Consulting or the Client. Such Confidential Information includes without limitation any information concerning Deloitte Consulting's or the Client's business, plans, operations, products, methods, procedures, customers, services, equipment, systems, and facilities and proprietary information, regardless of the form or method of communication.

   (b) Confidential Information shall be used by you only to the extent necessary for performance of the services and may be duplicated for or disclosed to only those persons within your organization having a need to know for purposes of performance of your services. You shall not disclose the Confidential Information to any third party and shall accord to all Confidential Information such protection as is necessary to prevent any other use, duplication, or disclosure, which protection shall be no less than a reasonable degree of care. Upon completion of performance or termination of the services, you shall deliver to Deloitte Consulting or its authorized representative all items embodying Confidential Information then in your possession or shall certify that all such items have been destroyed.

   (c) The restrictions set forth above shall apply, notwithstanding the completion or the termination of your services, until such time as you can establish that such information is known to the general public provided such knowledge is not due to your acts or omissions.

   (d) You have read, understood, and agree to comply with the Privacy Addendum attached hereto as Addendum A.

2. With respect to the work product prepared by you during the course of your services, you agree that:

   (a) Deloitte Consulting shall own all work product produced by you hereunder, including, without limitation, deliverables, computer programs (source code and object code), programming aids and tools, documentation, reports, data, designs, concepts, know-how, and other information, whether copyrightable or patentable or not (collectively, "Work Product"). Such work product shall be deemed to be "works made for hire." To the extent that any of the Work Product may not, by operation of law, be "works made for hire," you hereby assign to

Deloitte.

Deloitte Consulting all ownership rights, including, without limitation, intellectual property rights, in such Work Product. Deloitte Consulting shall have the right to obtain and hold copyrights, patent rights, registrations and similar protection which may be available for such work product. You agree to give Deloitte Consulting such assistance as may be reasonably required to perfect such rights.

(b) To the extent that any of your preexisting materials are contained in the Work Product, you hereby grant to Deloitte Consulting an irrevocable, worldwide, perpetual, royalty-free license to such preexisting materials. Such license includes, without limitation, the right to use, exe- cute, reproduce, display, perform, distribute (internally and externally) copies of, and prepare derivative works based upon, such preexisting materials and derivative works thereof. You acknowledge and agree that Deloitte Consulting may transfer such rights to others without your approval.

(c) Except for preexisting materials, you have no rights or license to use, publish, reproduce, prepare derivative works based upon, distribute, perform or display any Work Product.

(d) You warrant and represent (i) that the Work Product shall be your original work and will not infringe upon or violate any patent, copyright, trade secret, contractual or any other proprietary right of others; and (ii) that there exist no known rights, claims, causes of action or other legal rights or impediments.

(e) Your and Deloitte Consulting's rights and obligations in respect of all Work Product shall survive the completion or the termination of your services.

3. You agree that during your engagement to perform services hereunder and, to the extent permissible under applicable state law, for two years thereafter, you will not provide to Client or any contractor of Client, or solicit or offer to provide to Client or any contractor of Client, any software, services, or other products related to your services hereunder or the applicable Project without the advance written consent of Deloitte Consulting. You also agree that you will not make any public announcements, media releases, or other forms of public disclosure relating to your services, the Client, or the applicable Project without the advance written consent of Deloitte Consulting.

I acknowledge that I have read, that I understand, and that I agree to the foregoing.

Name: MOHAMMED NAWAZ

Signature: Mohammed Nawaz

Date: 07/06/2023

Subcontractor: DELOITTE

Client: State of Tennesse

Deloitte.

Addendum A

TO

Agreement Regarding Non-Disclosure of Information; Ownership of Work Product; Non-Compete

Privacy Addendum

This Privacy Addendum (this "Addendum") supplements and forms a part of the Subcontractor Agreement, dated as of _____, 202_, between Deloitte Consulting LLP ("Prime") and [Subcontractor] ("Subcontractor") (such agreement, the "Subcontractor Agreement", together with all attachments and exhibits thereto, including this Addendum and any schedules hereto, this "Agreement"). Capitalized terms used and not otherwise defined herein or in any schedule hereto shall have the meanings ascribed thereto in the Subcontractor Agreement.

If more than one security control requirement under this Addendum covers the same specific PII requirement to any Service in the Agreement, the requirement that is most protective to PII received by Subcontractor from Prime Contractor shall apply.

1. Definition of PII and Processing

"PII" means information relating to an identified or identifiable person that Prime Contractor or the Client provides to Subcontractor or that Subcontractor otherwise acquires from or on behalf of Prime Contractor, its affiliates, the Client or any of their respective personnel or agents in connection with the performance of services under this Agreement, whether in written, oral, electronic, or other form, and any copies thereof. It refers to refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as data and place of birth, mother's maiden name, etc. An "identified or identifiable person" is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier or one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity. "Processing" means any operation or set of operations performed on PII, such as accessing, obtaining, storing, transmitting, using, maintaining, disclosing or disposing of PII.

2. Using and Copying PII

Subcontractor shall Process PII only on the documented instructions of Prime Contractor, including those requirements of Exhibit C and the Statement of Work (SOW). Such instruction shall include Processing PII only for the specific purpose for which it was provided to Subcontractor and only reproducing PII to the extent reasonably necessary for these purposes.

3. Protection of PII

Subcontractor shall implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to (i) ensure the security and confidentiality of PII; (ii) protect against anticipated threats or hazards to the security or integrity of PII; and (iii) protect PII from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the Processing and the nature of the PII. Such safeguards shall meet federal standards for safeguarding PII, including but not limited to, OMB memoranda M-06-16 and M-07-16 and guidance from NIST, including NIST SP 800-53 (as revised), and NIST SP 800-122 Guide to Protecting the Confidentiality of PII.

Encryption. All transmissions between Subcontractor and Prime Contractor containing PII shall be encrypted. Encryption shall satisfy the standards for the applicable security level as specified in the Federal Information Processing Standard Publication 140-2 for data in motion and in NIST Special Publication 800-111 for data at rest. In furtherance, but not in limitation, of the foregoing, all PII received and stored by the Subcontractor shall be encrypted using AES128 Encryption as a minimum standard.

Massachusetts Law. To the extent that any PII relates to a resident of Massachusetts and constitutes "Personal

Information" as defined in 201 CMR 17.02 (as may be amended), Subcontractor shall also comply with the obligations of 201 CMR 17.00 et seq. (as may be amended), entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth", with respect to such PII.

Compliance with Laws. Without limiting the foregoing, Subcontractor shall comply with the confidentiality, privacy, and data security requirements of any law or regulation that is applicable to it in connection with the performance of services under this Agreement, including but not limited to, Federal Information Security Management Act ("FISMA"), 44 U.S.C. section 3541, et seq., the Privacy Act of 1974 (5 U.S.C. § 552a), and NIST SP 800-53.

4. Disclosure of PII

a) Except as otherwise agreed to in writing by the Parties, Subcontractor shall limit access to PII solely to its permitted subcontractors and those personnel of Subcontractor who have a need of such access in connection with the performance of the services under this Agreement, and shall not sell, disclose, release or otherwise make available PII to any other party. The disclosure of PII shall be limited to the specific information necessary for such subcontractors and personnel to perform the services under this Agreement. Subcontractor shall inform its personnel with access to PII of the requirements set forth in this Addendum and shall be responsible for its personnel's compliance with such requirements. Subcontractor will ensure that each of its subcontractors that has access to PII is bound by a written agreement requiring substantially the same obligations as Subcontractor under this Addendum and any relevant requirements from Exhibit C or the SOW. Subcontractor shall be responsible for its subcontractors' compliance with the terms of this Addendum.

b) Subcontractor will not be in violation of its obligations under the immediately preceding paragraph when PII is disclosed by Subcontractor to the extent required by an order of a court of competent jurisdiction or administrative agency, a validly enforceable subpoena, or any other legal or administrative process; provided that (i) Subcontractor provides prompt written notice to Prime Contractor of any such request or requirement with reasonably sufficient details regarding the request or requirement and the PII that Subcontractor is contemplating disclosing so that Prime Contractor and/or the Client may seek a protective order or other appropriate remedy and (ii) Subcontractor reasonably cooperates with Prime Contractor, its affiliates and/or the Client and their respective agents in connection with their efforts to seek such order or remedy.

5. Security Breach

Security Breach shall be governed by the terms of the Agreement including, but not limited, to any relevant requirements from Exhibit C or the SOW.

6. Disposal or Return of PII

Promptly upon the earlier of the completion of the services under this Agreement or the written request of Prime Contractor, all PII in any form, in Subcontractor's possession or under its control shall be returned to Prime Contractor (or at Prime Contractor's request, destroyed) without Subcontractor retaining any actual or recoverable copies thereof, in both instances without charge to Prime Contractor. Notwithstanding the immediately preceding sentence, Subcontractor may retain copies of PII to the extent required by applicable law and in accordance with Client requirements; provided that Subcontractor notifies Prime Contractor of the PII to be so retained.

7. Requests to Access and Correct PII

a) In the event that Subcontractor receives a request from a third party to access any PII in Subcontractor's possession, Subcontractor will promptly forward a copy of such request to Prime Contractor. Except as expressly permitted under Section 4 of this Addendum, Subcontractor shall not disclose any PII to a third party, whether in response to a request or otherwise.

b) Upon Prime Contractor's written request, Subcontractor will make PII in its possession available to Prime Contractor, or any third party designated in writing by Prime Contractor, and will correct PII in Subcontractor's possession in accordance with Prime Contractor's written instructions.

8. Information Requests

Deloitte.

Subcontractor will provide Prime Contractor with information as may be reasonably requested by Prime Contractor from time to time regarding Subcontractor's compliance with its obligations under this Addendum or otherwise relating to the Processing of PII.

9. Additional Information Related to EEA PII

If Subcontractor will Process PII related to individuals located in the European Economic Area, United Kingdom or Switzerland (collectively, "EEA PII"), the EU Standard Contractual Clauses adopted as European Commission Decision 2021/914/EU, as amended ("SCCs"), which can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, are incorporated by reference into this Addendum, and, with respect thereto, (a) Subcontractor will be a processor of Prime, (b) in the event that Prime is a controller, then Module 2 (controller to processor) shall apply, and in the event that Prime is a processor, then Module 3 (processor to processor) shall apply, (c) Clause 7 (Docking Clause) does not apply, (d) Subcontractor will consult and coordinate with Prime prior to notifying any third party about a personal data breach, (e) Subcontractor's use of sub-processors requires specific authorization by Prime (Clause 9(a), Option 1), which has been granted with respect to the sub-processors identified on Annex III to this Addendum, and Subcontractor shall provide at least 10 days advance notice of any additional requests for specific authorization, (f) the option in Clause 11(a) (Redress) does not apply, (g) the parties choose Option 1 of Clause 17, and agree these SCCs shall be governed by the law of the country (an European Economic Area member state, the United Kingdom or Switzerland; collectively "EEA/UK/CH") in which the entity is established that initially transferred the EEA PII out of the EEA/UK/CH, and per Clause 18(b) disputes arising under the SCCs shall be resolved in the courts of the same country, and (h) Annexes I, II, and III to this Addendum shall serve respectively as Annexes I, II, and III to the SCCs.

10. Noncompliance Notification and Remediation

In the event that Subcontractor determines at any time that it can no longer meet any of its obligations under this Addendum, Subcontractor shall promptly (a) notify Prime Contractor thereof and (b) take reasonable and appropriate steps to stop and remediate such noncompliance. In addition, if Subcontractor receives notice that it is not meeting any of its obligations under this Addendum, Subcontractor will take reasonable and appropriate steps to stop and remediate such noncompliance.

11. No Limitations of Liability

Notwithstanding anything in this Agreement to the contrary, the limitations and exclusions of liability set forth in this Agreement, if any, shall not apply to this Addendum and shall not limit Subcontractor's liability for failing to satisfy any of its obligations under this Addendum.

12. Survival

This Addendum shall survive the expiration or termination of this Agreement and thereafter remain in full force and effect for as long as Subcontractor or any of its subcontractors retains any PII; provided, however, Sections 5 and 8 of this Addendum shall survive indefinitely.

Deloitte.

TO BE COMPLETED ONLY WHEN EEA PII WILL BE PROCESSED (SEE SECTION 9 OF THE PRIVACY ADDENDUM)

DATA PROCESSING DETAILS FOR EEA PII

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s)

1. Name: Deloitte [insert entity name] LLP

Address: 30 Rockefeller Plaza, New York, NY 10112

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these Clauses: see Annex I, Section B below and the Agreement or applicable Statement of Work.

Signature and date: . . . . . .

Role (controller/processor): controller or processor depending on the specific data transferred

Data importer(s)

1. Name: . . . . . .

Address: . . . . . .

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these Clauses: see Annex I, Section B below and the Agreement or applicable Statement of Work.

Signature and date: . . . . . .

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Deloitte.

Categories of data subjects whose personal data is transferred

☐ Employees
☐ Dependents, beneficiaries, spouses, and/or domestic partners of employees
☐ Clients and customers
☐ Vendors or suppliers

Categories of personal data transferred

☐ Name
☐ Contact information such as telephone number, physical address, email address
☐ Employment information such as position, title, job description or personnel number
☐ Compensation and tax-related EEA PII
☐ Banking and financial account information
☐ Photos and videos
☐ Government-issued unique identifiers
☐ Gender
☐ Date of birth
☐ Internet log and tracking information, including cookies, beacons, IP addresses, and web browser and device information
☐ Online identifiers such as login and account information, including screen name, password and unique user ID
☐ Geolocation data
☐ Other:

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

☐ None
☐ EEA PII revealing racial or ethnic origin
☐ EEA PII revealing political opinions
☐ EEA PII revealing religious or philosophical beliefs
☐ EEA PII revealing trade union membership
☐ Genetic or biometric EEA PII
☐ Health or medical-related EEA PII
☐ EEA PII concerning a natural person's sex life or sexual orientation
☐ EEA PII relating to criminal convictions and offences

Applied restrictions and safeguards include limiting access to such personal data only to people who have a business need to access it, confidentiality training of Subcontractor's personnel, data minimization, and additional security measures set forth in Annex II.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

☐ One-off
☐ Continuous

☐ Other:

Nature of the processing

Data importer processes personal data in the context of providing the services to data exporter as set forth in the Agreement.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer and further processing is to enable the data importer to provide the services to data exporter as set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

While performing the services and as required by applicable laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Deloitte.

Processing by (sub)-processors in support of data importer related to the provision of the services to data exporter as set forth in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority/ies of the following countries: The supervisory authorities of the countries in which the entity is established that initially transferred the EEA PII out of the European Economic Area, the United Kingdom or Switzerland.

Deloitte.

TO BE COMPLETED ONLY WHEN EEA PII WILL BE PROCESSED (SEE SECTION 9 OF THE PRIVACY ADDENDUM)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Subcontractor will implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to (i) ensure the security and confidentiality of PII; (ii) protect against anticipated threats or hazards to the security or integrity of PII; and (iii) protect PII from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the Processing and the nature of the PII. These safeguards shall include, without limitation, a written information security plan; encryption of PII at rest and in transit; information access controls that require appropriate authorization, generate audit trails of approvals and require periodic reviews by asset owners; systems protections (e.g., intrusion protection); physical security measures; and a security awareness program, including employee training.

Deloitte.

TO BE COMPLETED ONLY WHEN EEA PII WILL BE PROCESSED (SEE SECTION 9 OF THE PRIVACY ADDENDUM)

ANNEX III
LIST OF AUTHORISED SUB-PROCESSORS

1. Name: . . . . . .
……..
Address: . . . . . .
……...
Contact person's name, position and contact details: . . . . . .
……..
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): . . . . . .
……

2. . . . . .
. . .

Deloitte.

TO BE COMPLETED ONLY WHEN REQUIRED PER SECTION 9 ABOVE

SCHEDULE 1
DATA PROCESSING DETAILS

SUBJECT MATTER AND DURATION OF THE PROCESSING:
The subject matter of the Processing is set out in this Agreement. The Processing will continue for so long as Subcontractor performs services under this Agreement or is authorized to Processes EEA PII pursuant to the terms of this Agreement.

NATURE AND PURPOSE OF THE PROCESSING:
Subcontractor provides Prime assistance with certain professional services, as further described in this Agreement.

TYPE OF EEA PII:
EEA PII Processed concerns the following categories of data: all categories of data related to the Processing associated with the professional services provided by Subcontractor for or on behalf of Prime, including the following:

X Name
X Contact information such as telephone number, physical address, email address
X Employment information such as position, title, job description or personnel number
X Compensation and tax-related EEA PII
X Banking and financial account information
X Photos and videos
X Government-issued unique identifiers
X Gender
X Date of birth
X Internet log and tracking information, including cookies, beacons, IP addresses, and web browser and device information
X Online identifiers such as login and account information, including screen name, password and unique user ID
X Geolocation data
X Special Categories of EEA PII:

☐ None
X EEA PII revealing racial or ethnic origin
X EEA PII revealing political opinions
X EEA PII revealing religious or philosophical beliefs
X EEA PII revealing trade union membership
X Genetic or biometric EEA PII
X Health or medical-related EEA PII
X EEA PII concerning a natural person's sex life or sexual orientation
X EEA PII relating to criminal convictions and offences

☐ Other:

CATEGORIES OF INDIVIDUALS TO WHOM THE EEA PII RELATES:

X Employees
X Dependents, beneficiaries, spouses, and/or domestic partners of employees
X Clients and customers
X Vendors or suppliers

OBLIGATIONS AND RIGHTS OF PRIME:
The obligations and rights of Prime are set forth in this Agreement.