1. Agreement – General Information and Term	
Agreement #	2026-BUS-7705
Title of Agreement ("Agreement")	Application Development, Maintenance, and Support for Managed IT Services
Cooperative or Public Entity	City of San Diego
Underlying Agreement #	City of San Diego MSA for ADMS
Underlying Agreement Website	https://www.sandiego.gov/purchasing/bids-contracts/gs
Start Date	As of the last signature below ("Effective Date")
End Date	March 1, 2031
Number of Annual Renewals	Five (5)
Use by Other Entities: This Agreement may be used by any entity authorized to purchase under this Agreement.	

2. Vendor Information			
Vendor:	**CGI Technologies and Solutions, Inc.**		
Sales Contact:	Matthew Fournie, VPCS	matthew.fournie@cgi.com 618-972-2714	
Contract Manager:	Amy Smith	amy.smith1@cgi.com 303 834 2643	
Addresses:	**Main Address:** CGI Technologies and Solutions Inc. 11325 Random Hills Road, 8th Floor Fairfax, VA 22030	**Billing Address:** CGI Technologies and Solutions Inc. 11325 Random Hills Road, 8th Floor Fairfax, VA 22030	**Notice Address:** CGI Technologies and Solutions Inc. 11325 Random Hills Road, 8th Floor Fairfax, VA 22030 Attn: Office of General Counsel US-OGC@cgi.com
SAM Unique Entity Identifier: VRJHEW8YZ2F5	**Iowa Secretary of State Business Number:** 184896	**Incorporated under the laws of:** DE	**Security Framework - Attachment B:** ISO 27001, ISO 27701, ISO 27017 & 27018, NIST Cybersecurity Framework 2.0, COBIT, NIS2, GDPR, AI Act and DORA

3. Agency Information		
Issuer:	**Iowa Department of Management ("DOM")**	
Contract Manager:		itcontracts@dom.iowa.gov
Addresses:	**Contact and Billing Address:** Department of Management Attn: Business Services 200 E. Grand Avenue, Ste.100 Des Moines, IA 50309 E: ITContracts@dom.iowa.gov	**Main and Formal Notice Address:** Department of Management Attn: Office of General Counsel 1007 E Grand Ave G13 Des Moines, IA 50319 email: domlegalnotices@iowa.gov

4. Master Agreement Summary

This Agreement governs the provision of information technology services to the State of Iowa and other eligible governmental entities, including but not limited to: application development, maintenance, and support; project management services; staff augmentation; infrastructure services; and consulting services.

5. Documents Incorporated/Order of Precedence

This Agreement and all attachments and external documents identified below are incorporated by this reference and together comprise the terms and conditions governing the relationship between the Parties, to be interpreted in the following order of precedence:

5.1. Ancillary agreements unique to a Purchasing Entity making purchases hereunder that specifically address state, local, or federal regulatory or compliance concerns and which may be incorporated via a Purchasing Instrument;

5.2. The following documents are incorporated by reference solely to establish their potential applicability and order of precedence. These documents shall apply to the extent expressly designated as applicable in a Purchasing Instrument executed hereunder. Inclusion of a reference in this section shall not, in itself, impose an obligation on Vendor unless and until such obligation is expressly incorporated into a Purchasing Instrument.

5.2.1. The IT Business Associate Agreement ("BAA"), which may be updated from time to time to conform with applicable federal laws, a current version of which is available at: https://dom.iowa.gov/media/222;

5.2.2. The IRS Publication 1075 Exhibit 7, which may be updated from time to time to conform with applicable laws, a current version of which is available at: https://www.irs.gov/pub/irs-utl/p1075.pdf ;

5.2.3. The Federal Certifications, which may be updated from time to time to conform to applicable federal law, a current version of which is available at https://dom.iowa.gov/media/377;

5.2.4. Iowa Code chapter 8F.

5.3. The terms of any Purchasing Instruments executed hereunder;

5.4. These General Terms and Conditions (Attachments A and B);

5.5. The Underlying Agreement;

5.6. RESERVED.

5.7. RESERVED

6. Signatures	
IN WITNESS WHEREOF, in consideration of the mutual covenants set forth above and for other good and valuable consideration, the receipt, adequacy, and legal sufficiency of which are hereby acknowledged, the Parties have caused their respective duly authorized representatives to execute this Agreement, which is effective as of the Effective Date.	
Vendor	**State of Iowa**
CGI Technologies and Solutions Inc.	**Department of Management**
Authorized signature: Matthew Fournie	**Authorized signature:** Kraig Paulsen
Date: 3/4/2026 | 12:44 PM CST	**Date:** 3/6/2026 | 11:07 AM CST
Printed Name: Matt Fournie	**Printed Name:** Kraig Paulsen
Title: VP Consulting Services	**Title:** Director, Department of Management
Address: 3 Cityplace Drive 11th floor St Louis, MO 63141	**Address:** 1007 E. Grand Ave. G13 Des Moines, Iowa 50309
Email: Matthew.Fournie@cgi.com	**Email:** ITContracts@dom.iowa.gov

Attachment A

General Terms and Conditions

The parties may be referred to herein individually as a **"Party"** or collectively as the **"Parties."** The Parties agree to the following:

1. Overview.

1.1. Reserved.

1.2. Relationship between this Agreement and Individual Purchasing Instruments. Each Purchasing Instrument executed hereunder shall be deemed, upon its execution, to incorporate the terms and conditions of this Agreement and shall constitute a separate, distinct, and independent Agreement between Vendor and the applicable Purchasing Entity. To the extent a Purchasing Entity other than DOM makes a purchase hereunder pursuant to a Purchasing Instrument executed by it, such Purchasing Entity shall be solely responsible for any payments due, duties, and obligations otherwise owed Vendor under the separate Purchasing Instrument. In addition, notwithstanding any other provision of this Agreement to the contrary, DOM bears no obligation or liability for any other Purchasing Entity's losses, liabilities, or obligations, including Vendor's failure to perform, arising out of or relating in any way to this Agreement. Likewise, the State of Iowa generally bears no obligation or liability for any political subdivision or other non-State Entity's losses, liabilities, or obligations, including the Vendor's failure to perform, arising out of or relating in any way to this Agreement.

1.3. Incorporation of the Underlying Agreement.

1.3.1. Governmental entities making purchases hereunder shall be afforded all of the rights, privileges, warranties, and indemnifications afforded by the Underlying Agreement, and such rights, privileges, warranties, and indemnifications shall accrue and apply with equal effect to governmental entities making purchases hereunder. Except as otherwise provided herein or in a Purchasing Instrument, Vendor shall perform all duties, responsibilities, and obligations required under the Underlying Agreement in the time and manner specified thereunder. In the event of any conflict or inconsistency between the terms and conditions of this Agreement and the Underlying Agreement, such conflict or inconsistency shall be resolved as stated on the CD&E.

1.3.2. Any references in the Underlying Agreement to the governmental entity or its governmental units, or to rights and privileges granted to such governmental units, shall be interpreted to mean the State of Iowa and its equivalent governmental entities for the purposes of this Agreement. Similarly, any references to the governmental entity statutes, regulations, case law, or other legal authorities shall be construed as references to the corresponding Iowa legal authorities addressing substantially similar subject matter.

2. Definitions. In addition to any other terms that may be defined elsewhere in this Agreement, the following terms shall have the following meanings:

2.1. **"AI"** or **"Artificial Intelligence"** means a machine-based system that is designed to autonomously or semi-autonomously generate or materially modify content, code, recommendations, or decisions that can influence physical or virtual environments. For

purposes of this Agreement, AI does not include incidental or embedded software features whose primary purpose is to assist with routine tasks (such as spell-check, grammar suggestions, or basic data sorting) and which do not independently generate or materially modify Deliverables under this Agreement.

2.2. **"Confidential Information"** means, subject to any applicable federal, state, or local laws and regulations, including Iowa Code Chapter 22, any confidential or proprietary information or trade secrets disclosed by either Party (**"Disclosing Party"**) to the other Party (**"Receiving Party"**) that, at the time of disclosure, is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the Parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include any information that: (i) was previously and rightfully in the possession of the Receiving Party from a source other than the Disclosing Party; (ii) was known to the Receiving Party prior to the disclosure of the information by the Disclosing Party; (iii) was disclosed to the Receiving Party without restriction by an independent third party having a legal right to disclose the information; (iv) is in the public domain; (v) is independently developed by the Receiving Party without any reliance on Confidential Information disclosed by the Disclosing Party; (vi) is disclosed or is required or authorized to be disclosed in compliance with applicable law; or (vii) is disclosed by the Receiving Party with the written consent of the Disclosing Party.

2.3. **"Customer Data"** means all information, data (including de-identified and aggregated data), materials, or documents (including Confidential Information and Personal Data) originating with, disclosed by, provided by, made accessible by, or otherwise obtained by or from the Purchasing Entity, the State of Iowa, or users, directly or indirectly, including from any Authorized Contractors of any of the foregoing, related to this Agreement in any way whatsoever, regardless of form, including all information, data, materials, or documents accessed, used, or developed by Vendor in connection with any Deliverables provided hereunder and all originals and copies of any of the foregoing.

2.4. **"Customer Property"** means any property, whether tangible or intangible, of or belonging to the Purchasing Entity, including Customer Data and Deliverables, software, hardware, programs, or other property possessed, owned, or otherwise controlled, maintained, or licensed by the Purchasing Entity, including third party software or third-party intellectual property.

2.5. **"DOM"** means the State of Iowa Department of Management and, unless the context clearly indicates otherwise, any independent contractors, consultants, or other third parties (including other governmental entities) who are retained, hired, or utilized by DOM in furtherance of this Agreement.

2.6. **"Personal Data"** means any information relating to an identified or identifiable person, including, but not limited to, Social Security or other government-issued identification numbers, federal or state tax information, "Personal Information" as defined in Iowa Code 715C, account security information, financial account information, credit/debit/gift or other payment card information, account passwords, intellectual property, document identification number, and sensitive or personal data (or equivalent terminology) as defined under any applicable law regarding privacy, data protection, information security obligations, or the Processing of Personal Data.

2.7. **"Process"** or **"Processing"** shall mean any operation or set of operations performed upon the Personal Data, whether or not by automatic means, including collection,

recording, organization, use, transfer, disclosure, storage, manipulation, combination, and deletion of Personal Data.

2.8. **"Purchasing Entity"** means the governmental entity that signs a Purchasing Instrument and, unless the context clearly indicates otherwise, any independent contractors, consultants, or other third parties who are retained, hired, or utilized by the Purchasing Entity in furtherance of the Purchasing Instrument or this Agreement.

2.9. **"Purchasing Instrument"** (also referred to as a "Statement of Work" or "SOW") means an individual transactional document executed hereunder for the purchase of Services or Deliverable(s) pursuant to this Agreement, regardless of form, and which identifies the specific Deliverable(s) to be purchased and any Acceptance Criteria or Specifications related thereto.

3. Modifications to the Underlying Agreement.

3.1. Schedules 1, 2, 3, 6, 7, 8, 10, 11, 12, 13, 14, 16, 17 are not incorporated into this Agreement.

3.2. Reference to "City" or "City of San Diego" shall mean the "State of Iowa," "DOM," or the applicable Purchasing Entity, as context requires.

3.3. References to "Client" shall mean the "State of Iowa," "DOM," or the applicable Purchasing Entity, as context requires.

3.4. References to "City Council" shall mean the relevant Iowa governmental authority having approval or oversight responsibility.

3.5. References to "City Data" shall mean "Customer Data" as defined is this Agreement.

3.6. References to California law, regulations, and authorities shall be construed as references to their Iowa equivalents.

3.7. Where the Underlying Agreement requires compliance with California-specific laws or regulations that have no Iowa equivalent or are inapplicable, such requirements shall be deemed satisfied if Vendor complies with all applicable Iowa and federal requirements addressing substantially similar subject matter.

3.8. Section 10.6 of the Underlying Agreement shall be struck in its entirety and replaced with the following:

> 10.6 Taxes. Vendor shall be responsible for paying any taxes incurred by Vendor in the performance of this Agreement. The State of Iowa, DOM, and the Purchasing Entity are exempt from the payment of sales and other taxes.

3.9. Section 16.1.1 (Limitation on Amount of City's Liability) is struck in its entirety and marked Reserved.

3.10. Sections 16.1.2 – 16.1.8 are struck in their entirety and replaced as follows:

> 16.1. Limitation of Liability. (a) The maximum aggregate liability of each Party under this Agreement, whether an action is in contract or tort and regardless of the theory of liability, shall be: (i) one (1) times the Contract Value of the Purchasing Instrument under which the liability arose ("General Damages Cap") for claims arising from Services, and (b) no party shall be liable to the other for

consequential, incidental, indirect, special, or punitive damages (including but not limited to consequential damages for the items listed in Section 16.3); provided, however, under no circumstances shall the foregoing limitations apply to damages, arising out of or relating to:

16.1.1. Intentional torts, criminal acts, fraudulent conduct, intentional or willful misconduct, or gross negligence;

16.1.2. Death, bodily injury, or tangible property damage;

16.1.3. Any contractual obligations pertaining to indemnification; intellectual property; liquidated damages; compliance with the applicable laws, rules, or regulations specifically identified in Section 21.1.8 ("Compliance with Laws") of this Agreement; or Confidential Information (which for clarity does not include Customer Data or Personal Data);

16.1.4. Claims arising under provisions of the Agreement calling for indemnification of the State for third-party claims against any the State for bodily injury to persons or for damage to real or tangible personal property caused by CGI's negligence or willful conduct. For clarity, this subsection 16.1.4 is only applicable if such provisions are specifically included in CGI's Indemnification Obligations in Section 22 of this Agreement.

16.2. Notwithstanding anything to the contrary in subsection 16.1, with the exception of those items set forth in Sections 16.1.1 through 16.1.3, CGI's aggregate liability for any and all claims, losses, liability, costs, and damages arising out of or relating to unauthorized disclosure of State Data (including Customer Data and Personal Data) due to CGI's failure to meet its security, privacy or disaster recovery obligations in this Agreement shall not exceed three times (3x) the Contract Value (the "Super Cap"). The parties agree that with respect to CGI's breach of its obligations in security, privacy or disaster recovery obligations in this Agreement and Attachment B resulting in the unauthorized disclosure of Customer Data or Personal Data the following items are deemed direct damages, and to the extent the State incurs such costs or expenses, CGI shall reimburse the Purchasing Entity subject to the Super Cap: (a) any forensic investigation to determine the cause of a security breach, and (b) notification of the security breach to applicable government and relevant industry self-regulatory agencies, to the media, and to individuals whose personal data may have been accessed or acquired.

16.3. The parties agree that any damages arising out of the following items shall be deemed consequential damages, and therefore, in no event will either party be responsible or liable with respect to any subject matter of this Agreement or terms and conditions related thereto under any contract, negligence, strict liability or other theory for: (a) error or interruption of use, loss, or inaccuracy or corruption of data, (b) cost of procurement of substitute goods, services, rights, or technology, or (c) any lost profits or revenues.

16.4. Acknowledged Direct Damages. The parties acknowledge and agree that the following types of damages shall be construed as direct damages and not as indirect, incidental, or consequential damages:

16.4.1 Reasonable costs and expenses that the State is required to incur during the ninety (90) day period immediately following a material default by CGI to procure reasonably comparable services from an alternative source or to provide such services itself, to the extent such costs and expenses exceed the fees the State would have paid CGI for such services under the applicable Purchasing Instrument during that period;

16.4.2 Reasonable costs and expenses of restoring, reconstituting, or recovering any Customer Data or State Data that is altered, damaged, lost, or corrupted as a result of CGI's failure to perform the Services in accordance with the performance standards and requirements set forth in this Agreement and the applicable Purchasing Instrument;

16.4.3 RESERVED.

16.4.4 Fines, penalties, or assessments imposed on the State by a federal or state regulatory authority as a direct result of and to the extent caused by CGI's failure to comply with laws, rules, or regulations applicable to its performance of Services under this Agreement, including but not limited to applicable requirements under IRS Publication 1075 and the FBI CJIS Security Policy, if any.

Sections 16.4.1 and 16.4.2 shall be subject to the General Damages Cap, and Section 16.4.4 shall be subject to the Super Cap. To the extent any damages described in this Section 16.4 also fall within the scope of Section 16.2, such damages shall be subject to the Super Cap set forth in Section 16.2 rather than the General Damages Cap.

16.5. Nothing in this Agreement, including this Section 16 (Limitation of Liability), shall be construed to waive any clause regarding the sovereign immunity of Customer or the State of Iowa.

16.6. The limitation of liability provisions set forth in this Section 16 are intended to comply with, and shall be interpreted consistently with, Iowa Administrative Code Rule 11-120.5. The exceptions to limitation of liability set forth in Rule 11-120.5(1) shall apply to this Agreement regardless of whether separately enumerated herein. To the extent any provision of this Section 16 is more restrictive of the State's rights or remedies than permitted under Rule 11-120.5, Rule 11-120.5 shall control. Nothing in Rule 11-120.5 shall be construed to reduce any liability obligation or cap set forth in this Section 16 that exceeds the minimum requirements of the Rule.

3.11. Section 14.2 (Termination by City for Convenience) shall be modified so that unless set forth in a SOW, fees are not incurred when exercising this provision.

3.12. Section 19 (Confidentiality) is struck in its entirety and marked Reserved. Confidentiality is governed by Attachment B and applicable law, including Iowa Code Ch. 22. In case of conflict, Attachment B controls for data protection measures; open-records obligations remain unaffected.

3.13. Section 21.1.3 (Conflict of Interest) shall be modified to include a subsection (i) that reads as follows:

21.1.3(i) To the extent applicable, the provisions of Iowa Code Chapter 68B shall apply to this Agreement and any Purchasing Instruments executed hereunder, and Vendor shall not engage in or permit any third party to engage in any conduct that would violate that chapter.

3.14. Section 22.1 (Indemnification by Vendor) shall be struck in its entirety and replaced with the following:

22.1. Indemnification Generally. Vendor and its successors and permitted assigns shall indemnify and hold harmless the State and their employees, officers, board members, agents, representatives, and officials ("Indemnitees") from and against any and all claims, actions, suits, liabilities, damages, losses, settlements, demands, deficiencies, judgments, fines, penalties, taxes, costs, and any other expenses (including the reasonable value of time of the Attorney General's Office and the reasonable costs, expenses, and attorney fees of other counsel retained by any Indemnitee) directly or indirectly related to, resulting from, or arising out of Vendor's performance under this Agreement, related to, resulting from, or arising out of third parties claims of:

22.1.1. Any personal injury or damage to real or tangible personal property caused, in whole or in part, by Vendor, Vendor Subcontractors, or Vendor Personnel related to the work performed or any Deliverables or the Services provided under this Agreement, including any Security Breach arising from the negligent act or omissions, intentional or willful misconduct, or unlawful acts of Vendor, Vendor Subcontractors, or Vendor Personnel;

22.1.2. Vendor, Vendor Subcontractors, or Vendor Personnel's failure to comply with any applicable local, state, and federal laws, rules, ordinances, regulations, standards, or orders in the performance of this Agreement, including, as applicable, Pub 1075 until such time as the State amends the Purchasing Instrument to no longer include Pub 1075 requirements;

22.1.3. Any claim for violation of any statutory or common law rights, including any claims or causes of action involving torts, or rights of privacy, confidentiality, misappropriation, or security, including any Security Breach, in each instance to the extent caused by the failure of Vendor, Vendor Subcontractors, or Vendor Personnel to comply with the terms of this Agreement. For the sake of clarity, each Party acknowledges and agrees that by entering into this Agreement, neither Party is assuming and should not be liable for the business and operational risks of the other Party's business. For the avoidance of doubt, the indemnification obligations in Sections 22.1.1 and 22.1.3 include third-party claims arising from Security Breaches to the extent such claims fall within the scope of those subsections.; or

22.1.4. Any claim for wages, benefits, compensation, insurance, discrimination, or other similar claims asserted against the State by any Vendor Personnel, or any claim, penalties, or fines made, levied, assessed, or imposed by another Governmental Entity against the State in any way related to or involving the misclassification of employees as independent contractors or any allegations or findings of the existence of a joint-employment relationship involving any Vendor Personnel.

22.2 Infringement Claim Additional Remedy. If a Deliverable becomes or is likely to become the subject of a claim that the Deliverable infringes a third party copyright, trade secret, trademark, mask work, United States patent, or other proprietary right, then, in addition to paying any damages and attorney fees as required above, Vendor may, at its sole option, either:

22.1.2.1 Promptly replace or modify the Deliverables, without loss of material functionality or performance, to make them non-infringing, or

22.1.5.2 Promptly procure for the Purchasing Entity the right to continue using the Deliverables.

If Vendor finds that neither of these alternatives is available to it on commercially reasonable terms, Vendor may be required to terminate Indemnitees' access to the infringing item and/or Indemnitees shall be required to return the infringing item. In the event Vendor terminates the Indemnitees' access to an infringing item pursuant to this Section, Vendor shall (i) refund to the State a pro-rated amount (in cash or by means of a credit) of the pre-paid but unused Fees paid for the infringing Deliverable or, if the infringing item is a component of a larger Deliverable, a proportionate share of the pre-paid fees attributable to the infringing component, and (ii) reimburse the State for documented, reasonable costs incurred to procure a replacement for the lost functionality, not to exceed the fees refunded under clause (i).

Any costs associated with implementing either of the above alternatives will be borne by the Vendor.

22.3 Vendor's indemnification obligations specified in this Agreement are conditioned upon the Indemnitees promptly notifying the Vendor in writing of the proceeding, providing the Vendor a copy of all notices received by the Indemnitees with respect to the proceeding, cooperating with the Vendor in defending or settling the proceeding, and allowing the Vendor to control the defense, selection of attorneys, and settlement of the proceeding to the extent permitted by Law. At its own expense, Indemnitee may observe the proceeding and confer with counsel of its choice. To the extent required by Law, the Indemnitee shall have the right to participate in its own defense through a representative of the Iowa Department of Justice. Settlement offers made on behalf of the Indemnitee purporting to bind it must be approved by the Indemnitee, provided that such approval will not be unreasonably withheld. Vendor will not be obligated to indemnify or defend, or be liable for costs or damages, under this Section 22.3 to the extent the infringement arises out of: (i) modifications made to the item in question by anyone other than Vendor and its subcontractors working at Vendor's direction; (ii) the combination, operation or use of the item with other items Vendor did not supply; (iii) Indemnitees failure to use any new or corrected versions of the item made available by Vendor; or (iv) Vendor's adherence to Indemnitees' specifications or instructions.

3.15. Section 23.3 (Specific Requirements) shall be modified to include a subsection (j) that reads as follows:

23.3(j) Certificates of Coverage. The Vendor shall submit certificates of the insurance, which indicate coverage and notice provisions as required by this

Contract, to the Agency upon execution of this Contract. Send the Certificate of Insurance (COI) to the DOM contract email address: **ITContracts@dom.iowa.gov**. Include in the COI the following additions:

COI - Description of Operations box shall state:

The State of Iowa and the Iowa Department of Management are named as additional insured. Vendor shall give at least thirty (30) days prior written notice of any insurance cancellation to the State of Iowa and the Iowa Department of Management.

COI - The Certificate Holder box shall state:

State of Iowa - Department of Management
200 East Grand Avenue
Des Moines, IA 50309

3.16. Section 24 (Dispute Resolution) shall be struck in its entirety and replaced with the following:

At the written request of either party, the parties will attempt to resolve any dispute arising under or relating to the Agreement through the informal means described in this Section 24. Each party will appoint a senior management representative who does not devote substantially all of his or her time to performance under the Agreement. The representatives will negotiate in an effort to resolve the dispute without the necessity of any formal proceeding. The parties express their mutual preference for resolving disagreements through the informal process described in this Section before resorting to formal proceedings where circumstances reasonably permit. The parties agree that, where circumstances reasonably permit, a party will allow thirty (30) calendar days from the date of a written request to negotiate before commencing formal proceedings. This thirty-day period is intended as a good-faith expectation and does not operate as a condition precedent to initiating formal proceedings. Either party may commence formal proceedings at any time without first exhausting the informal process described in this Section. The parties shall continue good-faith negotiations during any such proceedings unless otherwise ordered by the court. Informal dispute resolution is non-binding and does not operate as a precondition to any formal proceeding. Nothing in this Section shall limit the rights of the Attorney General set forth in Iowa Code, Title 1, Chapter 13, Section 27.11 (Governing Law; Venue) is struck in its entirety and replaced with the following:

27.11 Choice of Law and Forum. This Agreement shall be governed by the laws of the State of Iowa, without giving effect to the choice of law principles of Iowa law. Any litigation in connection with this Agreement shall be brought and maintained in the state or federal courts sitting in Polk County, Iowa.

4. Additional Provisions.

4.1. Purchasing Instruments. A Purchasing Entity executing a Purchasing Instrument pursuant to this Agreement may agree to additional terms and conditions in a Purchasing Instrument that are in conflict with or inconsistent with the terms and conditions of this

Agreement. Such Purchasing Instrument terms apply only to the scope of work identified in the Purchasing Instrument and do not alter the agreed terms in this Agreement. Notwithstanding the foregoing, the following terms of this Agreement shall always control regardless of any contrary terms that may be in a Purchasing Instrument:

4.1.1. The administrative information contained in Sections 1-5 of the CD&E;
4.1.2. The definition of Confidential Information;
4.1.3. Set-off obligations in Section 10.4 of the Underlying Agreement;
4.1.4. Compliance with laws in Section 21.1.8 of the Underlying Agreement;
4.1.5. Conflict of interest obligations in Section 21.1.13 of the Underlying Agreement;
4.1.6. Termination provisions in Section 14 of the Underlying Agreement.

4.2. No Additional Fees. Unless agreed upon in writing, the Purchasing Entity shall not be obligated to pay amounts to Vendor that include travel, lodging, and related expenses. In no event shall the Purchasing Entity be responsible for payment of Vendor's performance costs incurred in connection with this Agreement, including but not limited to equipment, supplies, personnel, salaries, benefits, insurance, training, conferences, telephone, utilities, start-up costs, and all other operational and administrative costs and expenses. To the extent any Purchasing Instrument calls for reimbursement of travel, such travel charges may never exceed the amounts allowed under DAS-SAE travel policy, DAS-SAE Title 210. (available at: https://das.iowa.gov/state-employees/travel-and-relocation/210-travel). For vendors, travel reimbursement may not exceed the amounts that would be payable under DAS-SAE 210.245. (available at: https://das.iowa.gov/sites/default/files/acct_sae/sae_manual/210/210-245.pdf). In addition, in-state lodging reimbursement is limited to providers certified by the Iowa Department of Public Safety's Human Trafficking Prevention Training.

4.3. Invoice Submission. Vendor shall submit all invoices for payment to the Purchasing Entity by August 1 for all services performed in the preceding state fiscal year (the State fiscal year ends June 30). If the Vendor seeks payment for end of state fiscal year claims submitted after August 1, the Vendor may submit the late claims, but the Purchasing Entity will only reimburse the claims if funding is available and the Purchasing Entity is legally authorized to make payment. If funding is not available after the end of the state fiscal year, the Vendor may submit the claim to the Iowa State Appeal Board for a final decision regarding reimbursement of the claim.

4.4. Retention. To secure Vendor's performance under this Agreement, a Purchasing Entity may retain a mutually agreed upon percentage of the fees or other compensation associated with each Deliverable provided under a Purchasing Instrument (**"Retained Amounts"**) until all Deliverables under such Purchasing Instrument have been provided and the Purchasing Entity has given its Final Acceptance. Retained Amounts shall be payable upon the Purchasing Entity's delivery of written notice of Final Acceptance, subject to the terms and conditions hereof.

4.5. Vendor Performance Monitoring.

4.5.1. DOM monitors performance through a Vendor scorecard program that collects data on Vendor performance under state contracts gathered through a formal feedback process. Feedback may address cost, delivery and support, flexibility, partnership, and security and compliance. Performance data may include the Vendor's effectiveness in meeting contract obligations, service level agreements, project management requirements, and risk management protocols.

4.5.2. Vendors have access to their scorecard results and the methodology by which they are calculated. Scorecards are typically issued annually during the term of the contract. DOM reserves the right to publicly post vendor scorecard results, except where a low score is anticipated, in which case the Vendor will be notified in advance and given the opportunity to appeal through DOM's established process for contested cases applicable to vendor appeals in the applicable Iowa Administrative Code.

4.5.3. Scorecard performance may be considered in relation to future State purchasing decisions.

4.6. Use of Artificial Intelligence.

4.6.1. Advance Approval for AI Usage. Vendor shall obtain prior written approval from the Purchasing Entity before utilizing artificial intelligence (AI) technologies in the provision of services under this Agreement or Purchasing Instruments entered into pursuant to this Agreement. The Vendor shall clearly identify in writing the specific AI technologies to be employed, their intended functions, and their potential impact on service delivery.

4.6.2. Documentation of AI Utilization. In cases where computer code is generated, written, or modified using AI technologies, the Vendor shall ensure that the sections of code influenced by AI are thoroughly documented with appropriate comments indicating that they are the result of AI utilization. This Documentation shall be provided along with any Deliverables that include AI-derived code.

4.6.3. AI Training Data Usage. The Vendor shall not employ Customer Data or Confidential Data to train AI systems without obtaining prior written approval from the Purchasing Entity. The intended usage of such data for AI training must align with existing data usage rights, and the Vendor shall ensure that data privacy and security are maintained throughout the process.

4.6.4. Data Normalization to Prevent Discrimination. The Vendor shall include within a submitted Plan of Action and Milestones (POAM) a detailed outline of the measures to be taken for data normalization in AI training. This normalization process shall be designed to prevent algorithmic discrimination and ensure fair and equitable outcomes.

4.6.5. Evaluation of Third-Party AI Offerings. Should the Vendor intend to employ third-party AI offerings in the execution of this Agreement or Purchasing Instruments entered into pursuant to this Agreement, the Vendor must provide a comprehensive explanation of how such AI technologies have been trained to avoid algorithmic discrimination, safeguard data privacy, and ensure system safety and effectiveness. The Vendor shall also provide advanced notice and clarification to any individuals whose data might be used for future AI training.

4.6.6. Human Alternatives and Fail-Safe Mechanisms. In instances where AI technologies fail to adequately fulfill the service requirements, the Vendor shall ensure the provision of human-operated alternatives that are capable of meeting the needs of the circumstance. These alternatives shall be readily available to ensure seamless service continuity.

4.6.7. Human Vetting of AI Output. Prior to finalizing any output generated by AI technologies, the Vendor shall subject such output to thorough human evaluation

and interaction. This evaluation shall assess the accuracy, relevance, and appropriateness of AI-generated content, ensuring the delivery of high-quality, reliable results. Any AI-generated or materially modified code must undergo human technical review, SAST/DAST, supply an SBOM, and pass change-control; AI shall not operate in mission-critical workflows without independent validation.

4.6.8. Compliance and Reporting. The Vendor shall adhere to all applicable laws, regulations, and standards governing the use of AI technologies applicable to the provision of Services in the context of the Agreement. The Vendor shall provide regular reports to the Purchasing Entity detailing the usage, performance, and outcomes of AI technologies as per the terms of this clause.

4.7. Administrative Fees and Reporting.

4.7.1. Vendor shall provide one percent (1.00%) administrative fee on all sales made through this Agreement, without affecting authorized prices/rates. This one percent (1.00%) administrative fee shall be paid quarterly to the Iowa Department of Management, Attn: Chief Financial Officer, at the billing address located in CD&E section. Payment shall be made in accordance with the following schedule:

Period End	Reporting and Fee Due
September 30 (Q1)	October 31
December 31 (Q2)	January 31
March 31 (Q3)	April 30
June 30 (Q4)	July 31

4.7.2. The Vendor shall submit a quarterly report via email to **ITContracts@dom.iowa.gov** detailing all sales in the State of Iowa and identifying the Purchasing Entity, the Purchasing Instrument number, and the State of Iowa Contract number. The quarterly sales report is due on the dates listed above.

Attachment B - Data Protection Addendum

1. Definitions:

1.1. **"Security Breach"** means the loss of control, compromise, unauthorized use, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses personally identifiable information; or an authorized user accesses Customer Data for a reason other than an authorized purpose.

1.2. **"Security Incident"** means an occurrence that actually jeopardizes the confidentiality, integrity, or availability of (1) Customer Data, and/or (2) an information system or the information the system Processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Notwithstanding the foregoing, routine, blocked reconnaissance activity (e.g., commodity port scans) shall not constitute a reportable Security Incident unless such activity escalates to include successful footholds, or data access anomalies.

2. Confidentiality

2.1. Customer Data. The Purchasing Entity owns and has exclusive rights to all Customer Data. Vendor must treat all Customer Data as Confidential Information, keep it secure, and not disclose or use it for any purpose other than providing goods or services under the Agreement. All uses for commercial or political purposes are strictly forbidden. Vendor must comply with any restrictions on use or disclosure outlined in the Agreement or applicable law. Vendor may only retain Customer Data for purposes of performing pursuant to the Purchasing Instrument or by prior written approval of the Purchasing Entity. The Vendor may be held civilly or criminally liable for improper use or disclosure of Customer Data. The Vendor shall not link any data provided by DOM or a Purchasing Entity with any other data systems or data sets without prior written permission from the applicable entity.

2.2. Vendor Confidential Information. Unless otherwise required by applicable law, the Purchasing Entity will not intentionally disclose Vendor's Confidential Information to a third party (excluding the Purchasing Entity's Authorized Contractors) without the Vendor's prior written consent.

2.3. Return or Destruction. Upon completion of duties under this Agreement or upon the specific direction of either party, the other party shall return or destroy Confidential Information and/or Customer Data and not retain any copies thereof, subject to any retention obligations imposed by law. If immediate destruction is not possible, the party retaining such information shall return or destroy the retained information as soon as feasible and shall certify that the retained information will be safeguarded to prevent unauthorized disclosures until it has been purged. Once all Confidential Information and/or Customer Data has been completely purged, the party purging the information shall provide certification of destruction in accordance with methods approved by the National Institute of Standards and Technology.

2.4. Compelled Disclosures. In the event that a subpoena or other legal process is served upon either party for Customer Data held by Vendor or for Vendor Confidential Information held by a Purchasing Entity, the party shall promptly notify the other party and cooperate in any lawful effort to defend against the disclosure.

2.5. Open Records and Electronic Discovery Requests. Vendor must assist the Purchasing Entity by providing information needed to comply with open records laws (including Iowa Code Chapter 22) or in connection with any legal process or proceeding. Vendor's assistance in this regard must be provided timely and designed to meet the timing obligations imposed by law. Vendor will ensure Customer Data is stored and maintained so as to avoid spoliation or other electronic discovery issues.

3. Security/Privacy.

3.1. Data Protection. Vendor shall safeguard the confidentiality, integrity, and availability of Customer Data, Customer Property, and the Deliverables. In so doing, Vendor shall implement and maintain reasonable and appropriate administrative, technical, and physical security measures to safeguard against unauthorized access, disclosure, theft, or modification of Customer Data, Customer Property, and Deliverables.

3.2. Compliance with Security Plan. Vendor represents and warrants that it will adhere to the cybersecurity plan adopted pursuant to the Vendor Security Framework identified in the CD&E. Vendor will ensure that its internal policies, procedures, and practices align with the objectives and requirements set forth in the cybersecurity plan and the Vendor Security Framework. The identified Vendor Security Framework may be changed or updated from time to time by mutual agreement of the Parties.

3.3. Compliance Reporting. Once each calendar year during the Term, DOM may request, and Vendor shall provide, evidence of compliance with the Vendor's Security Framework and an annual SOC 2 Type II or equivalent, and pen-test executive summaries, plus bridge letters in each case limited in scope to how these relate to the Services provided under this Agreement,

3.4. Encryption. Customer Data shall be encrypted at rest and in transit with controlled access, and the Deliverables shall use TLS 1.2 or higher. Unless otherwise expressly provided herein or otherwise agreed to by the Parties in writing, Vendor is responsible for encryption of Customer Data in its possession. Additionally, Vendor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in Federal Information Processing Standards (FIPS) 140-3, Security Requirements for Cryptographic Modules for all Customer Data, unless the Purchasing Entity approves in writing the storage of Customer Data on a portable device that does not satisfy these standards.

3.5. CONUS Obligation. Access, storage, Processing, transmission, retention, or other maintenance of Customer Data at rest and all backups shall occur solely in the continental United States of America. Vendor shall not allow Vendor Personnel to access, store, Process, or retain Customer Data on any portable devices, including personal computers, tablets, or cell phones, except to the extent such devices are used and permanently stored or backed up at all times only in the continental United States of America.

3.6. Import and Export of Data. Purchasing Entity must have the ability at all times to extract Customer Data and other information from any Vendor systems housing such information or data. Vendor must assist with such extracts when necessary, must not interfere with such extracts, must ensure extracts are provided at no additional charge to the Purchasing Entity, and must make sure that data can be exported in a commercially reasonable format so that the Purchasing Entity can then import data into other systems. Regarding exporting data and information, the Vendor must ensure that the Purchasing Entity receives the requested data or information within seven days of making a request. The format of the exported data should be as specified by the Purchasing Entity or, if not feasible, in a commercially reasonable format.

3.7. Security Audits. During the Term, if Vendor is providing dedicated hosting services, DOM or the Purchasing Entity may engage a neutral, independent, third-party auditor to perform security audits of Vendor's dedicated hosting environment used to provide Deliverables. Vulnerabilities will be measured using standards set forth at https://cve.mitre.org/. Vendor agrees to remediate vulnerabilities identified through such audits within the following timeframes: (a) Critical vulnerabilities: 15 days; (b) Serious vulnerabilities: 30 days.

3.8. Access to Security Logs and Reports. If Vendor is providing dedicated hosting services, Vendor shall provide security logs and reports to DOM and/or the Purchasing Entity in a mutually agreeable format upon request. Such reports shall include, at minimum, latency statistics, user access summaries, user access IP address summaries, and user access history and security logs related to Customer Data. If Vendor is providing dedicated hosting services, Vendor shall provide tenant-scoped access logs (user IDs, timestamps, source IPs), administrative action logs, and security event summaries related to Customer Data, with redactions for other tenants limited in scope to how these relate to the Services provided under this Agreement.

3.9. Personnel Safeguards.

3.9.1. *Background Checks.*

3.9.1.1. *Minimum Requirements*. Vendor shall comply with its internal background check policies. Where Vendor does not have an internal background check policy, or in the event Vendor's background check policy is inadequate based on the nature of Customer Data stored or processed by Vendor, Vendor agrees to comply with DOM background check policy. Vendor shall provide DOM and the Purchasing Entity with these background check results in a mutually agreeable form and manner prior to Vendor staff performing services pursuant to this Agreement or a Purchasing Instrument. In the event of an adverse finding, Vendor Personnel may be disqualified from performing services under the Agreement in the sole discretion of the applicable Purchasing Entity.

3.9.1.2. *Costs.* Vendor is responsible for all costs associated with any Vendor Personnel background checks, regardless of who performs the background checks.

3.9.1.3. *Additional Screening*. If any Vendor Personnel will access, or have the ability to access, data that is subject to federal regulatory requirements (including, but not limited to, data regulated under the Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) Security Policy, Internal Revenue Service (IRS) Publication 1075, or other federal data protection laws), then the Vendor shall ensure that such personnel undergo background checks in compliance with all applicable federal regulations prior to the commencement of any engagement involving access to such data.

These background checks may include, as required by the applicable regulations, a work history review, financial review, state or local criminal history check, and a national criminal history check through the Federal Bureau of Investigation (FBI). Vendor Personnel may also be required to authorize the release of background check results, including

those from the FBI, to DOM, the Purchasing Entity, or other applicable governmental authorities.

Such background checks may be conducted by the Purchasing Entity, DOM, or their Authorized Contractors, or may be required to be performed by Vendor (to the extent Vendor is authorized) in accordance with applicable federal standards. The results shall be provided in a mutually agreeable form and manner prior to access to the regulated data.

DOM and the Purchasing Entity reserve the right to require additional background screening during the engagement, consistent with applicable law and regulation.

3.9.1.4. *Operational Requirements for CJIS and IRS 1075 Engagements.* For any engagement requiring access to data subject to the CJIS Security Policy or IRS Publication 1075, the following operational requirements apply in addition to the requirements of Sections 3.9.1.1 through 3.9.1.3:

3.9.1.4.1. *Fingerprinting Process.* Unless otherwise agreed in the applicable Purchasing Instrument, Vendor Personnel requiring access to CJIS or FTI data shall submit to fingerprint-based criminal history record checks administered through the State's designated submission process. Vendor shall coordinate with DOM or the Purchasing Entity to schedule fingerprint submissions. The State or its authorized agent shall receive and maintain all fingerprint submission results.

3.9.1.4.2. *(b) Clearance Gating.* No Vendor Personnel shall be granted access to CJIS or FTI data, systems, or environments until the fingerprint-based background check has been completed and the individual has been affirmatively cleared. Provisional or temporary access pending completion of background checks is prohibited.

3.9.1.4.3. *(c) Adjudication.* DOM or the Purchasing Entity shall adjudicate background check results in accordance with the applicable CJIS Security Policy or IRS Publication 1075 requirements. Vendor Personnel with disqualifying criminal history under the applicable federal standard, as interpreted by DOM or the Purchasing Entity in its sole discretion, shall not be permitted to access CJIS or FTI data.

3.9.1.5. *Right to Remove Individuals.* The Purchasing Entity and DOM shall have the right at any time to require that the Vendor remove from interaction with the Purchasing Entity or DOM, as applicable, any Vendor representative performing Services on a time and materials basis who the Purchasing Entity or DOM reasonably believes is detrimental to its working relationship with the Vendor. The Purchasing Entity or DOM will provide the Vendor with written notice of its determination and the reasons it requests the removal. If the Purchasing Entity or DOM signifies that a potential security violation exists with respect to the request, the Vendor shall promptly remove such individual. The Vendor shall not

assign the person to any aspect of this Agreement or future work orders without the Purchasing Entity's or DOM's consent.

3.9.2. *Security Awareness Training.* Vendor Personnel providing services to DOM or a Purchasing Entity are required to attend annual security awareness training addressing the importance of securing, safeguarding, and otherwise appropriately handling Customer Property, including Customer Data. Any such security awareness training shall minimally conform with applicable DOM Security Awareness Training policies or requirements. Where a Purchasing Instrument requires compliance with training requirements imposed by federal partners, the Vendor agrees to comply with the more stringent training requirements.

3.9.3. *Separation of Job Duties and Non-disclosure.* Vendor shall monitor and enforce separation of job duties, and limit access to and knowledge of Customer Property and Customer Data to those Vendor Personnel to which such access and knowledge is necessary to provide the Deliverables hereunder. Vendor Personnel may be required to sign the Purchasing Entity's standard confidentiality or non-disclosure agreement(s), or other confidentiality or non-disclosure agreement(s), including as may be required by applicable law, rule, regulation, or policy.

4. Security Incidents and Breaches.

4.1. Security Incident or Data Breach Notification:

4.1.1. *Reporting Requirements.* Vendor must report Security Incidents and Security Breaches (collectively "Security Events") to the contact identified in the applicable Purchasing Instrument(s) as well as to the State of Iowa Security Operations Center ("SOC"):

Email: soc@iowa.gov
Local: 515-281-4762 (4SOC)

4.1.2. *Notification Timeframes.* The Vendor shall notify the SOC of Security Events within the shorter of (a) 72 hours, (b) the timeframe listed in the Purchasing Instrument, or (c) the timeframe imposed by applicable law. Vendor shall only delay notification to DOM and the Purchasing Entity of a Security Event when required to do so by applicable law.

4.2. Investigations in Response to Security Events. The Vendor agrees at its sole expense to take all steps necessary to promptly remedy any Security Event and to fully cooperate with DOM and the Purchasing Entity in investigating and mitigating any damage from such Security Events. Upon notice of any Security Event, the Vendor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the Security Event. As soon as practicable during the investigation, the Vendor will deliver to the SOC a Security Event assessment and the Vendor's plans for future mitigation. When DOM notifies Vendor that the investigation into any Security Event has concluded, Vendor will deliver to DOM and the Purchasing Entity a final root cause assessment and future incident mitigation plan as soon as practicable. Vendor agrees that it will not notify any regulatory authority relating to any Security Event unless DOM and the Purchasing Entity specifically request Vendor do so in writing, or unless otherwise required to do so by applicable law.

4.3. Consumer Notification Obligation. DOM or the Purchasing Entity shall be responsible for all applicable consumer notification requirements in the event of a Security Event caused in whole or in part by Vendor.

4.4. Exposure for Damages related to Security Events. Vendor, subject to the Limitation of Liability in Section 16.1 of the Underlying Agreement, as amended by this Agreement shall be responsible for all damages arising directly or indirectly, in whole or in part, out of any Vendor breach of its obligations related to a Security Event.

5. Disaster Recovery and Business Continuity.

5.1. Creation, Maintenance, and Testing. If Vendor provides hosting Services, the Vendor shall maintain a Business Continuity and Disaster Recovery Plan for the Deliverables ("**Plan**"), test the Plan at least yearly, and implement the Plan in the event of any unplanned interruption. The Plan, compliance history, and testing results may be accessed by 1) a Vendor hosted virtual meeting to discuss Vendor policies and procedures, 2) provide DOM or the Purchasing Entity a copy of our Security Baseline Overview which provides a detailed overview of Vendor's security program and policies or 3) at DOM's expense, bring printed copies to DOM's offices to be reviewed in person. In addition, DOM reserves the right to inspect, or to engage a neutral, independent third-party auditor approved by DOM, to review the Vendor's Disaster Recovery and Business Continuity Plan, compliance history, and testing results. Vendor shall cooperate fully with such inspections or audits, provided that any proprietary information disclosed shall be subject to a mutually agreed NDA. Throughout the Term, the Vendor shall maintain disaster avoidance procedures designed to safeguard the Customer Data, the data processing capability, and the availability of the Deliverables. Additional disaster recovery and business continuity requirements may be set forth in individual Purchasing Instruments.

5.2. Activation of Plan. The Vendor shall immediately notify DOM and the Purchasing Entity of any disaster or other event that results in the activation of the Plan. If Vendor fails to reinstate the Deliverables impacted by any such disaster within the periods of time set forth in the Plan, DOM or Purchasing Entity, as applicable, may immediately terminate this Agreement or applicable Purchasing Instrument as a non-curable breach and without any penalty or liability. Termination under this section is in addition to any other remedies available hereunder. Force Majeure provisions of the Agreement shall not limit Vendor's obligations under this section.

5.3. Backup and Recovery. Except as otherwise set forth in a Purchasing Instrument or Service Level Agreement, if the Vendor's Services include hosting, the Vendor shall maintain a contemporaneous backup of Customer Data such that the data shall be restored within twenty-four hours at any point in time. Additionally, unless otherwise provided in a Purchasing Instrument or applicable Service Level Agreement, Vendor shall store a backup of Customer Data in a facility at least as secure as the production facility no less than daily, and maintain the security of Customer Data consistent with the security requirements set forth in this Agreement. Backups of Customer Data shall not be considered in calculating storage used by DOM or a Purchasing Entity in the event that fees are calculated based on storage used or amount of data transfer under the Agreement. All costs of data restoration shall be borne by the Vendor.

6. Survives Termination. Vendor's duties, obligations, and liabilities as set forth in this Data Protection Addendum shall survive termination of this Agreement.