

PARTICIPATING ADDENDUM NO. 9412

AMENDMENT NO. 3

This is Amendment No. 3 to Participating Addendum No. 9412 effective April 1, 2019, as amended from time to time ("Participating Addendum") between the State of Oregon, acting by and through its Department of Administrative Services ("DAS"), on behalf of state agencies and members of the Oregon Cooperative Purchasing Program ("Authorized Purchaser") and Carahsoft Technology Corp. ("Contractor"). This Amendment is effective upon signature by the parties ("Amendment Effective Date").

The parties agree to amend the Participating Addendum, as follows:

1. Section 1.6 of the Participating Addendum is hereby deleted and replaced in its entirety with the following:
 - 1.6 Order of Precedence. In the event of a conflict between the terms and conditions of this Participating Addendum and its Exhibits or the Master Agreement, the following order of precedence applies:
 - 1.6.1 This Participating Addendum, less its exhibits;
 - 1.6.2 Exhibit B - State Specific Terms and Conditions;
 - 1.6.3 Exhibit F - State of Oregon Information Security Terms;
 - 1.6.4 Exhibit H - Publication 1075 Exhibit 7: Safeguarding Contract Language;
 - 1.6.5 Exhibit A – Products and Pricing;
 - 1.6.6 The Master Agreement, including its attachments;
 - 1.6.7 Exhibit C – Required Insurance;
 - 1.6.8 Exhibit E – Vendor Management Provisions;
 - 1.6.9 Exhibit D – VCAF and VSR; and
 - 1.6.10 Exhibit G – Independent Contractor Certification
2. Section 8.4.4 of the Participating Addendum is deleted and replaced in its entirety with the following:
 - 8.4.4. Section 6103 of the Internal Revenue Code and guidance issued by the Internal Page 10 of 75 Revenue Service with respect to compliance thereof, including IRS Publication 1075 or its replacement, as amended from time to time, and the terms and conditions set forth in Exhibit H; and
3. Exhibit B, Section 1.1 is deleted and replaced in its entirety with the following:
 - 1.1. Documents; Order of Precedence. In the event of a conflict between the terms and conditions of this Contract and its Exhibits or the Master Agreement, the following order of precedence applies:
 - 1.1.1. The Participating Addendum, less its exhibits;
 - 1.1.2. The Purchase Order
 - 1.1.3. These State of Oregon Participating Addendum Terms and Conditions;
 - 1.1.4. Exhibit F - State of Oregon Information Security Policies and Terms;
 - 1.1.5 Exhibit H - Publication 1075 Exhibit 7: Safeguarding Contract Language;
 - 1.1.6. Exhibit A – Products and Pricing
 - 1.1.7. The Master Agreement, including its attachments;
 - 1.1.8. Exhibit C – Required Insurance;
 - 1.1.9. Exhibit E – Vendor Management Provisions

- 1.1.10. Exhibit D – VCAF and VSR; and
- 1.1.11. Exhibit G – Independent Contractor Certification

4. Exhibit B 5.4.4. is deleted and replaced in its entirety with the following:

5.4.4 Section 6103 of the Internal Revenue Code and guidance issued by the Internal Revenue Service with respect to compliance thereof, including IRS Publication 1075 or its replacement, as amended from time to time, and the terms and conditions set forth in Exhibit H; and

- 5. Exhibit F, Part I, Information Security, the URL for the State of Oregon Statewide Security Standards is hereby deleted and replaced with the following:
<https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf>
- 6. Exhibit H, Publication 1075 Exhibit 7: Safeguarding Contract Language, attached hereto, is hereby made a part of the Participating Addendum.

Except as expressly amended above, all other terms and conditions of the Participating Addendum are still in full force and effect. Contractor certifies that the representations, warranties and certifications contained in the Participating Addendum are true and correct as of the Amendment Effective Date and with the same effect as though made at the time of execution of the Participating Addendum.

Certification: The individual signing on behalf of Contractor hereby certifies under penalty of perjury: (a) the number shown on this form is Contractor’s correct taxpayer identification; (b) Contractor is not subject to backup withholding because (i) Contractor is exempt from backup withholding, (ii) Contractor has not been notified by the IRS that Contractor is subject to backup withholding as a result of a failure to report all interest or dividends, or (iii) the IRS has notified Contractor that Contractor is no longer subject to backup withholding; (c) s/he is authorized to act on behalf of Contractor, s/he has authority and knowledge regarding Contractor’s payment of taxes, and to the best of her/his knowledge, for a period of no fewer than six calendar years preceding the Amendment Effective Date, Contractor has faithfully has complied with and is not in violation of: (i) all tax laws of this state, including but not limited to ORS 305.620 and ORS chapters 316, 317, and 318;(ii) any tax provisions imposed by a political subdivision of this state that applied to Contractor, to Contractor’s property, operations, receipts, or income, or to Contractor’s performance of or compensation for any work performed by Contractor; (iii) any tax provisions imposed by a political subdivision of this state that applied to Contractor, or to goods, services, or property, whether tangible or intangible, provided by Contractor; and (iv) any rules, regulations, charter provisions, or ordinances that implemented or enforced any of the foregoing tax laws or provisions; and;. (d) Contractor is an independent contractor as defined in ORS 670.600; and (e) the supplied Contractor data is true and accurate.

CONTRACTOR:

THE STATE OF OREGON, acting by and through the Department of Administrative Services

By: Kristina Smith

By: Debbie Davis

Title: Contracts Director

Title: IT Procurement Strategist

Date: 9/29/2022

Date: 9/29/2022

FEID: 52-2189693

Approved pursuant to ORS 291.047
By: John McCormick via email dated 9/28/2022
Senior Assistant Attorney General

Exhibit H

Publication 1075 Exhibit 7: Safeguarding Contract Language

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- (1) All work will be performed under the supervision of the Contractor.
- (2) The Contractor and Contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The Contractor will certify that FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this Contract will be subcontracted without the prior written approval of the IRS.
- (9) Contractor will ensure that the terms of FTI safeguards described herein are included,

without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the agency under this Contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and obligated to the agency under this Contract.

(12) For purposes of this Contract, the term "Contractor" includes any officer or employee of the Contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1),

provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a Contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A Contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.