This Fourth Amendment to Oklahoma Statewide Contract No. 1041 (the "Fourth Amendment") is effective as of the date of the last signature below, between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and Carahsoft Technology Corporation ("Supplier"). This Fourth Amendment supplements and amends the Oklahoma Statewide Contract No. 1041 with Carahsoft Technology Corporation entered into by the parties and effective on October 26, 2023, (the "Agreement"), including all supplements and amendments thereto. Unless otherwise indicated, capitalized terms used in this Fourth Amendment without definition shall have the respective meanings specified in the Agreement.

For good and valuable consideration, the parties agree as follows:

1. Supplier and State agree the following attachment is incorporated hereto:

   Attachment A: Amendment to Reseller Agreement – Carahsoft Technology Corporation and Salesforce, Inc.

2. The attached Reseller Agreement shall apply to all Salesforce's lines of business off ordered off SW1041 with Carahsoft Technology Corporation including but not limited to MuleSoft, Slack, and Tableua.

3. Except as expressly modified by this Fourth Amendment, all terms and provisions of the Contract not addressed herein remain as executed by the parties and in full force and effect.

4. The Fourth Amendment may be executed in multiple counterparts, each of which will be an original and together will constitute the same instrument.

SIGNATURES

The undersigned represent and warrant that they are authorized, as representatives of the Party on whose behalf they are signing, to sign this Fourth Amendment and to bind their respective Party thereto.

STATE:	**SUPPLIER:**
Joe McIntosh (May 29, 2024 09:59 CDT)	Stephen Dickerson
Authorized Signature	**Authorized Signature**
Joe McIntosh	Stephen Dickerson
Printed Name	**Printed Name**
CIO	Sales Manager
Title	**Title**
May 29, 2024	May 28, 2024
Date	**Date**

AMENDMENT TO RESELLER AGREEMENT

This Amendment to the Reseller Agreement ("Amendment") is entered into and effective as of the last date beneath the parties' signature below ("Amendment Effective Date"), by and between Salesforce, Inc., (f/k/a salesforce.com, inc.) ("SFDC") and Carahsoft Technology Corporation ("Reseller"). SFDC and Reseller entered into the Amended and Restated Reseller Agreement with an effective date of August 21, 2020, as amended ("Agreement"). SFDC and Reseller now mutually agree to amend the Agreement as set forth in this Amendment solely for the benefit of the State of Oklahoma. For clarity, the Customer is Carahsoft's customer.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. IRS Publication 1075 Requirements. Exhibit A to this Amendment, Safeguarding Contract Language – IRS Publication 1075 Exhibit 7, is hereby added to the Agreement for the benefit of Carahsoft's Customer.

2. Social Security Administration Requirements. Exhibit B to this Amendment, Social Security Administration ("SSA") Requirements, is hereby added to the Agreement for the benefit of Carahsoft's Customer.

3. Except as specifically provided for by this Amendment, the Agreement is unmodified and shall remain in full force and effect.

IN WITNESS WHEREOF, Reseller and SFDC have executed this Amendment as of the Amendment Effective Date.

RESELLER

Signature: Stephen Dickerson

Print Name: Stephen Dickerson

Title: Sales Manager

Date: 2/14/23

SALESFORCE, INC.

Signature: DocuSigned by: Santiago Parra 753C910EDD1D484...

Print Name: Santiago Parra

Title: Manager, Order Management

Date: 2/13/2023

Exhibit A

Safeguarding Contract Language

IRS Publication 1075, Exhibit 7

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:

i. All work will be performed under the supervision of the contractor.

ii. 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. SFDC employees do not have logical access to unencrypted FTI unless such access is specifically allowed by Customer. In the event that the Customer has a need to grant such access to an SFDC employee for support purposes, Customer will first notify SFDC in writing and verify that the employee has completed a fingerprint-based background check in compliance with the requirement in IRS Publication 1075.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

x. 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. For clarity, SFDC as a subcontractor shall assume toward the contractor, Carahsoft Technology Corporation ("Carahsoft"), the obligations, duties and responsibilities as set forth in the Master Reseller Agreement executed between SFDC and Carahsoft, the customer-specific amendment thereto pertaining to the State of Oklahoma, including this Exhibit 7, and Order Forms issued by SFDC to Carahsoft identifying State of Oklahoma agencies as the End Customer.

xi. 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. For clarity, SFDC as a subcontractor is obligated to perform the services in accordance with the approved subcontract, which consists of the Master Reseller Agreement executed between SFDC and Carahsoft, the customer-specific amendment thereto pertaining to the State of Oklahoma, including this Exhibit 7, and Order Forms issued by SFDC to Carahsoft identifying State of Oklahoma agencies as the End Customer.

xii. 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. SFDC will use a third party infrastructure cloud service provider in performance of the Services ("sub-processor"), and such sub-processor shall not have logical access to FTI. Sub-processor is not a "subcontractor" as defined herein.

xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein and does not cure within thirty (30) days.

xiv. In the event the IRS determines this Exhibit is insufficient to address compliance with IRS Publication 1075, Exhibit 7, Carahsoft, the State of Oklahoma, and Salesforce agree to negotiate in good faith to resolve the SSA's concerns."

II. CRIMINAL/CIVIL SANCTIONS

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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 IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, 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. 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. For clarity, with regard to SFDC and its sub-processor, SFDC shall afford, with notice, the IRS and the Agency, as defined in IRS Publication 1075, access to SFDC's technical capabilities, documentation, records, and databases, to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of IRS Publication 1075 protected data. SFDC provides this clarification as the facilities, installations, operations and/or infrastructure for which may be identified in Section III. Inspection are provided by a third party as SFDC's infrastructure cloud service provider, and subject to the policies of said third party. Furthermore, SFDC requests that any inspections are

conducted in a manner designed to minimize disruption of SFDC's normal business operations and complies with the terms and conditions of all data confidentiality, ownership, privacy, security, and restricted use provisions of the contracts between the parties. Where the IRS is not a party to the contract, SFDC will inform the IRS of the applicable data confidentiality, ownership, privacy, security, and restricted use provisions of such contracts applicable to the inspection.

Exhibit B

Social Security Administration ("SSA") Requirements (If applicable to SSA-provided information uploaded to Salesforce Government Cloud Plus)

a. PERFORMANCE: In performance of this Agreement, the Contractor (Carahsoft) and its supplier (Salesforce) agree to comply with and assume responsibility for compliance by their respective employees with the following requirements:

i. All work will be done under the supervision of the Contractor or the Contractor's employees or Salesforce and its employees.

ii. Any data received or accessed by a State of Oklahoma agency under the IEA identified in subsection viii below and provided to Salesforce ("the SSA-provided information") shall be used by Salesforce only in connection with providing the Salesforce Services to the State of Oklahoma consistent with the SFDC Terms of Use, the Salesforce Documentation and this Exhibit. Such information 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 Agreement. Inspection by or disclosure to anyone other than an officer or employee of the Contractor or Salesforce (or sub-processors consistent with subsection iv below) is prohibited.

iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving SSA-provided information furnished under this Agreement shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA. Salesforce will use a third party infrastructure cloud service provider in performance of the Services ("sub-processor"), and such sub-processor shall not have logical access to Customer Data. Sub-processor is not a "subcontractor" for purposes of this Exhibit. As of the effective date of this Agreement, the Salesforce Services branded as Government Cloud Plus has FedRAMP High Provisional Authority to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board. The Security, Privacy, and Architecture document applicable to Government Cloud Plus is available at:

https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/government-cloud-plus-security-privacy-and-architecture.pdf.

v. The Contractor shall maintain a list of employees authorized access to SSA-provided data in logical, unencrypted form. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA. Salesforce employees will not have logical, unencrypted access to SSA-provided information unless a State of Oklahoma agency grants access to a specific Salesforce employee to login to a specific state agency org within the Salesforce platform. The State of Oklahoma agency will be able to track such access and provide a list of any such employees to the SSA.

vi. Contractor or Salesforce or agents thereof may not legally process, transmit, or store SSA-provided information in a cloud environment, nor shall the State of Oklahoma place any SSA-provided information into the cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to Salesforce by the applicable State of Oklahoma agency prior to uploading any SSA-provided information to the Salesforce Services. Salesforce shall not have any liability in the event

that the State of Oklahoma uploads SSA-provided information without authorization from SSA. The State of Oklahoma shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training.

vii. Salesforce requires its employees who have access to the Government Cloud Plus environment to sign a non-disclosure agreement upon hire, and such employees are required to comply with the privacy, data protection, and data security and training requirements applicable to the Government Cloud Plus environment. Salesforce shall retain non-disclosure agreements in accordance with Salesforce's record retention schedule, which as of the Effective Date of this Agreement, for informational purposes and may be subject to change, is five (5) years after the term of employment for each such employee.

viii. The State of Oklahoma provided the Contractor and Salesforce with a copy of the Information Exchange Agreement and its six related attachments executed between the State of Oklahoma Department of Human Services and the SSA and effective as of December 1, 2022 (collectively the "IEA") prior to execution of this Agreement. Salesforce is a Cloud Service Provider as defined in the IEA Agreement rather than a "contractor" or "agent".

ix. In the event that an Oklahoma state agency provides a Salesforce employee with unencrypted, logical access to SSA-provided information, the role and function of such employee shall be to provide technical support / help desk support to the Oklahoma state agency with the Salesforce platform.

x. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA- provided information.

xi. SSA requires all parties subject to this Agreement to agree that any State of Oklahoma owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the State of Oklahoma and is subject to onsite inspection and review by the State of Oklahoma or SSA with prior notice. For clarity, with regard to SFDC and its sub-processors, SFDC shall afford, with notice, SSA and authorized representatives of the State of Oklahoma, access to SFDC's technical capabilities, documentation, records, and databases, to the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of SSA-provided data. SFDC provides this clarification as the facilities, installations, operations and/or infrastructure are provided by a third party as SFDC's infrastructure cloud service provider and subject to the policies of said third party. Furthermore, SFDC requests that any inspections are conducted in a manner designed to minimize disruption of SFDC's normal business operations and complies with the terms and conditions of all data confidentiality, ownership, privacy, security, and restricted use provisions of the contracts between the parties. Where SSA or the State of Oklahoma is not a party to the contract, SFDC will inform the State of Oklahoma and SSA of the applicable data confidentiality, ownership, privacy, security, and restricted use provisions of such contracts applicable to the inspection.

xii. For purposes of this section, "Security Breach" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to SSA-provided information uploaded to the Services as Customer Data. In the event that Salesforce reasonably suspects that a

Security Breach has occurred and initiates an investigation of said occurrence or if a Security Breach is verified to have occurred, Salesforce shall notify the relevant Salesforce Services system administrator designated by the State Oklahoma agency without undue delay, and in any event within 24 hours. The obligations herein shall not apply to Security Breaches that are caused by the State of Oklahoma or its users, although to the extent Salesforce is aware, Salesforce shall use reasonable efforts to notify the State of Oklahoma of a Security Breach caused by the State or its users. In addition, if the applicable state agency maintains an email address for a security contact in the Salesforce Services ("Security Contact"), Salesforce will use commercially reasonable efforts to notify the State of Oklahoma by emailing that Security Contact. The applicable State of Oklahoma state agency is responsible for maintaining the accuracy and currency of the Security Contact.

xiii. The State of Oklahoma shall have the right to void this Agreement if the Contractor fails to provide the safeguards described above and does not cure within thirty (30) days.

xiv. In the event the SSA determines this Exhibit is insufficient to address cloud service provider requirements of the IEA, Carahsoft, the State of Oklahoma, and Salesforce agree to negotiate in good faith to resolve the SSA's concerns.

Execution Version Amendment Four - SSA and PUB 1075 Salesforce

Final Audit Report 2024-05-29

Created:	2024-05-23
By:	Courtney Templeton (courtney.templeton@omes.ok.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWvGlifYhrur5H47YtddJXOxB85xiJzJZ

"Execution Version Amendment Four - SSA and PUB 1075 Sale sforce" History

Document created by Courtney Templeton (courtney.templeton@omes.ok.gov)
2024-05-23 - 11:11:25 PM GMT

Document emailed to Stephen Dickerson (stephen.dickerson@carahsoft.com) for signature
2024-05-23 - 11:12:21 PM GMT

Email viewed by Stephen Dickerson (stephen.dickerson@carahsoft.com)
2024-05-28 - 6:20:28 PM GMT

Document e-signed by Stephen Dickerson (stephen.dickerson@carahsoft.com)
Signature Date: 2024-05-28 - 6:21:40 PM GMT - Time Source: server

Document emailed to Joe McIntosh (joe.mcintosh@omes.ok.gov) for signature
2024-05-28 - 6:21:42 PM GMT

Document e-signed by Joe McIntosh (joe.mcintosh@omes.ok.gov)
Signature Date: 2024-05-29 - 2:59:19 PM GMT - Time Source: server

Agreement completed.
2024-05-29 - 2:59:19 PM GMT