BOARD OF SUPERVISORS AGENDA ITEM REPORT
AWARDS / CONTRACTS / GRANTS

○ Award ◉ Contract ○ Grant

Requested Board Meeting Date: 8/13/2024

** = Mandatory, information must be provided*

or Procurement Director Award: ☐

***Contractor/Vendor Name/Grantor (DBA):**

Carahsoft Technology Corp.

***Project Title/Description:**

Computer Software and Related Items

***Purpose:**

Amendment of Award: Master Agreement No. MA-PO-24-078, Amendment No. 03. This Amendment extends the termination date to 09/30/2024, and incorporates the Snowflake Terms and Conditions for Snowflake software and related services. No additional funds needed at this time. Administering Department: Information Technology

***Procurement Method:**

Pursuant to Pima County Procurement Code 11.24.010, Cooperative procurement authorized, on 11/21/2023, the Board of Supervisors approved an award of contract for an initial term effective 11/21/2023 to 12/31/2023 in the annual award amount of $2,000,000.00 with two (2) one-year renewal options.

On 03/11/2024, the Procurement Director approved Amendment No. 01, which executed a partial renewal option to extend the termination date to 03/31/2024. No additional funds required. One (1) renewal option remained.

On 04/04/2024, the Procurement Director approved Amendment No. 02, which executed a partial renewal option to extend the termination date to 06/30/2024. No additional funds required. One (1) renewal option remained.

PRCUID: 504704

Attachment: Contract Amendment No. 03

***Program Goals/Predicted Outcomes:**

Expand the Pima County Information Technology Department's (ITD) ability to fulfill the Countywide software and related needs by the addition of an additional software reseller source.

***Public Benefit:**

Permitting ITD to source software needs from multiple resellers allows ITD to obtain the multiple price quotes, and ensure third party software terms comply with Arizona Statutory requirements.

***Metrics Available to Measure Performance:**

Continuity and consistency of business operations. ITD will require quotes from all vendors to obtain best possible pricing and more efficient purchasing timelines.

***Retroactive:**

Yes, contract could not be extend until the State of Arizona extended the parent cooperative contract.

To: COB 07/26/24
VRS: N/A
Pgs: 9

THE APPLICABLE SECTION(S) BELOW MUST BE COMPLETED
Click or tap the boxes to enter text. If not applicable, indicate "N/A". Make sure to complete mandatory (*) fields

Contract / Award Information

Document Type: _____ Department Code: _____ Contract Number (i.e., 15-123): _____

Commencement Date: _____ Termination Date: _____ Prior Contract Number (Synergen/CMS): _____

☐ Expense Amount $ _____* ☐ Revenue Amount: $ _____

***Funding Source(s) required:** _____

Funding from General Fund? ○ Yes ○ No If Yes $ _____ % _____

Contract is fully or partially funded with Federal Funds? ○ Yes ○ No

If Yes, is the Contract to a vendor or subrecipient? _____

Were insurance or indemnity clauses modified? ○ Yes ○ No
If Yes, attach Risk's approval.

Vendor is using a Social Security Number? ○ Yes ○ No
If Yes, attach the required form per Administrative Procedure 22-10.

Amendment / Revised Award Information

Document Type: MA Department Code: PO Contract Number (i.e., 15-123): 24-078

Amendment No.: 03 AMS Version No.: N/A

Commencement Date: 07/01/24 New Termination Date: 09/30/24

Prior Contract No. (Synergen/CMS): N/A

◉ Expense ○ Revenue ○ Increase ○ Decrease Amount This Amendment: $ 0.00

Is there revenue included? ○ Yes ◉ No If Yes $ _____

***Funding Source(s) required:** General Fund and Enterprise Fund

Funding from General Fund? ◉ Yes ○ No If Yes $ _____ % 50

Grant/Amendment Information (for grants acceptance and awards) ○ Award ○ Amendment

Document Type: _____ Department Code: _____ Grant Number (i.e., 15-123): _____

Commencement Date: _____ Termination Date: _____ Amendment Number: _____

☐ Match Amount: $ _____ ☐ Revenue Amount: $ _____

***All Funding Source(s) required:** _____

***Match funding from General Fund?** ○ Yes ○ No If Yes $ _____ % _____

***Match funding from other sources?** ○ Yes ○ No If Yes $ _____ % _____

***Funding Source:** _____

***If Federal funds are received, is funding coming directly from the Federal government or passed through other organization(s)?**

_____

Contact: Procurement Officer, Fred LeVeque Acting Division Manager, Troy McMaster

Department: Procurement Director, Terri Spencer Telephone: 520.724.8728

Department Director Signature: Javier Baca Date: 07/23/2024

Deputy County Administrator Signature: _____ Date: 7-25-24

County Administrator Signature: _____ Date: 7/26/2024

Pima County Procurement Department

Project: Computer Software and Related Items

Contractor: Carahsoft Technology Corp.
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

Contract No.: MA-PO-24-078

Contract Amendment No.: 03

Orig. Contract Term:	11/21/2023 – 12/31/2023	**Orig. Amount:**	$ 2,000,000.00
Termination Date Prior Amendment:	03/31/2024	**Prior Amendments Amount:**	$ 0.00
Termination Date This Amendment:	09/30/2024	**This Amendment Amount:**	$ 0.00
		Revised Total Amount:	$ 2,000,000.00

CONTRACT AMENDMENT

The parties agree to amend the above-referenced contract as follows:

1. **Background and Purpose.**

   1.1. Background. On November 21, 2023, County is extending the contract term. County and Contractor entered into the above referenced agreement to provide software and software services that are available through Contractor's catalog.

   1.2. The Contract incorporated State of Arizona Contract CTR046098, which has been extended through September 30, 2024.

   1.3. Purpose. County is extending the contract term. County is amending the Contract to incorporate the third-party terms and conditions required to use certain software purchased under this Contract.

2. **Term.** The Parties agree to extend the current extension option for three additional months commencing on July 1, 2024, and terminating on September 30, 2024. If the commencement date is before the Effective Date of this amendment, the parties will, for all purposes, deem the amendment to have been in effect as of the commencement date.

3. **Snowflake Terms & Conditions.** This Amendment incorporates **Exhibit A: Carahsoft Quote # 41249725** (2 pages) & **Exhibit B: Snowflake CJIS Access Terms Addendum** (5 pages) into the Contract**.** The terms in **Exhibits A** & **B** apply only to the Snowflake software and services referenced in **Exhibits A** & **B.**

4. **Third-Party Beneficiary**. Per Section 4 of the Contract Snowflake, Inc. ("Snowflake") is considered a Third-Party Beneficiary and not a direct party to the Contract.

SIGNATURE PAGE TO FOLLOW

All other provisions of the Contract not specifically changed by this Amendment remain in effect and are binding upon the parties.

PIMA COUNTY

Chair, Board of Supervisors

Date

CARAHSOFT TECHNOLOGY CORP.

Natalie LeMay

Authorized Officer Signature

Natalie LeMay, State & Local Contracts Manager

Printed Name and Title

6/27/2024

Date

ATTEST

Clerk of the Board

Date

APPROVED AS TO FORM

Deputy County Attorney

Rachelle Barr 07/17/2024

Print DCA Name

CONTRACT
NO. MA-PO-24-078
AMENDMENT NO. 03
This number must appear on all invoice, correspondence and documents pertaining to this contract.

The contents of this contract are confidential. Requests for a copy shall be submitted to the Clerk of the Board by completing a Public Records Request pursuant to County Administrative Procedure 4-4. The Public Records Request form can be located at http://webcms.pima.gov/ under the 'Quick Links' section. Release of confidential contract information involves a process above and beyond the basic Public Records Request process. This process will be performed by the Procurement Department after the Clerk of the Board receives the completed Public Records Request.

If you have any questions, please call (520)724-8161.

EXHIBIT B

Snowflake CJIS Access Terms Addendum

Last Updated: August 16, 2023

THIS SNOWFLAKE CJIS ACCESS TERMS ADDENDUM (this "**CJIS Access Terms Addendum**") between You and Reseller (each individually a "**Party**" and collectively the "**Parties**") governs Your access to and use of the Snowflake CJIS Service and CJIS Ancillary Services to upload, process, store, or transmit Customer Data that qualifies as CJI. This CJIS Access Terms Addendum supplements and amends the Snowflake U.S. SnowGov Region Access Terms ("**U.S. SnowGov Region Access Terms**"), and is effective as of the date the last Party signs this CJIS Access Terms Addendum ("**CJIS Access Terms Addendum Effective Date**"). Unless otherwise defined in this CJIS Access Terms Addendum, all capitalized terms used and not defined herein will have the meanings ascribed to them in the U.S. SnowGov Region Access Terms, the Use Terms or Documentation. You represent and warrant that you are authorized to bind the business, government entity, or government agency, on whose behalf you are accepting this CJIS Access Terms Addendum (such entity hereinafter, "**You**", "**Your**", or "**you**"). The right granted under this CJIS Access Terms Addendum are expressly conditioned upon such authority and acceptance.

For good and valuable consideration, the sufficiency of which both Parties acknowledge, the Parties hereby agree as follows:

1. **New Defined Terms**.

   a. "**CJI**" or "**Criminal Justice Information**" has the meaning used in the CJIS Security Policy.
   b. "**CJIS**" means Criminal Justice Information Services.
   c. "**CJIS Audit**" is defined in Section 3(d) of this CJIS Access Terms Addendum.
   d. "**CJIS Security Addendum**" means the uniform CJIS Security Addendum approved by the Attorney General of the United States, as referenced in 28 C.F.R. § 20.33(a)(7), and attached as Exhibit H to the CJIS Security Policy.
   e. "**CJIS Security Policy**" means the CJIS Security Policy published by the U.S. Department of Justice, Federal Bureau of Investigation, CJIS Division in effect as of the CJIS Access Terms Addendum Effective Date.
   f. "**CJIS Covered Accounts**" means Your Accounts in the applicable Service in which You store and process Customer Data within the CJIS Regions in which You have indicated, by signing this CJIS Access Terms Addendum, Your intent to upload, process, store, or transmit Customer Data that qualifies as CJI.
   g. "**CJIS Regions**" mean the Snowflake regions that are expressly designated by Snowflake as meeting the requirements for compliance with the CJIS Security Policy, as set forth in the Documentation.
   h. "**Contracting Government Agency**" is defined in the CJIS Security Addendum.
   i. "**Covered Snowflake Personnel**" is defined in Section 3(b) of this CJIS Access Terms Addendum.
   j. "**Covered Snowflake Personnel Screening Information**" is defined in Section 4(d) of this CJIS Access Terms Addendum.
   k. "**Security Incident**" as defined in Section 7 (Incident Detection & Response) of the Snowflake Security Addendum (available at www.snowflake.com/legal-gov) has the same meaning as "security violation" in the CJIS Security Addendum.
   l. "**Snowflake CJIS Service**" means the Service when used within a CJIS Region in accordance with this CJIS Access Terms Addendum.
   m. "**CJIS Ancillary Services**" means the Technical Services (including any Deliverables), support, and other services to prevent or address service or technical problems in connection with the Snowflake CJIS Service.

2. **Applicability and Scope.**
   a. **Applicability.** Subject to the terms in this CJIS Access Terms Addendum and the U.S. SnowGov Region Access Terms, You may use Your CJIS Covered Accounts to upload, process, store, or transmit Customer Data that qualifies as CJI.

b. **SCOPE.** Notwithstanding anything to the contrary in this CJIS Access Terms Addendum, the U.S. SnowGov Region Access Terms and/or the Use Terms, all commitments to You are made exclusively by Reseller (and not Snowflake Inc. or any of its Affiliates (collectively, "**Snowflake**")), and You must look solely to Reseller regarding any rights, claims or damages relating to, or arising out of, the Service, the Use Terms, this CJIS Access Terms Addendum and/or the U.S. SnowGov Region Access Terms. Reseller is not an agent of Snowflake and is not acting on behalf of Snowflake, and You are not a third-party beneficiary to any agreement between Reseller and Snowflake.

3. **Reseller Obligations.**

a. **CJIS Security Policy.** In accordance with this CJIS Access Terms Addendum and subject to the assignment of responsibilities hereunder and in the U.S. SnowGov Region Access Terms and Documentation, Snowflake maintains a security program consistent with the applicable requirements of the CJIS Security Policy and the terms of the CJIS Security Addendum, in each case with respect to Your CJIS Covered Accounts. In the event of additions or changes to the CJIS Security Policy, CJIS Security Addendum, or other applicable policies and standards established by the CJIS Advisory Policy Board, Snowflake will use commercially reasonable efforts to update and maintain the safeguards described in its security program consistent with any such compliance requirements applicable to Snowflake within the prescribed timelines. For clarity, where security controls are under Your control (e.g., configurations of CJIS Covered Accounts and User access thereto), You are responsible for implementing and maintaining those controls to meet applicable requirements.

b. **Covered Snowflake Personnel.** Subject to Section 4(d) of this CJIS Access Terms Addendum:

i. Snowflake will meet the personnel training and location requirements set out in the CJIS Security Policy as applicable to CJI with respect to Snowflake personnel that, in the ordinary course of providing the Snowflake CJIS Service and CJIS Ancillary Services (as described in the Documentation), have the ability to access unencrypted Customer Data that qualifies as CJI stored in CJIS Covered Accounts ("**Covered Snowflake Personnel**"). Covered Snowflake Personnel each receive the CJIS Security Addendum and the CJIS Security Policy and execute an acknowledgement of such receipt and the content of the CJIS Security Addendum.

ii. Covered Snowflake Personnel have each been successfully screened by a state CJIS Systems Agency in accordance with the screening requirements set out in the CJIS Security Policy as applicable to CJI. If You elect to screen the Covered Snowflake Personnel to satisfy Your own screening procedures, such screening of the Covered Snowflake Personnel that You perform will be subject to Section 4(d)(ii) of this CJIS Access Terms Addendum.

c. **Incident Notification and Response**.

i. You will be notified of Security Incidents with respect to CJIS Covered Accounts in accordance with Section 7 of the Snowflake Security Addendum (available at www.snowflake.com/legal-gov).

ii. In the event You are not the Contracting Government Agency, You shall carry out any required notifications under the CJIS Security Policy and CJIS Security Addendum, including to the Contracting Government Agency and appropriate third parties.

d. **You and Third Party Audits.**

i. Snowflake will reasonably cooperate with You and third parties authorized under the CJIS Security Policy in the event an investigation, inquiry, or audit in connection with Your CJIS Covered Accounts that is lawfully conducted pursuant to Section 5.11 of the CJIS Security Policy or Sections 4 or 5 of the CJIS Security Addendum ("**CJIS Audit**"), provided that:

1. You shall send a reasonably scoped, written request for such CJIS Audit to Snowflake not less than 30 business days prior to the desired start date for such CJIS Audit, unless prohibited from doing so by the CJIS Security Policy.

2. To the extent permitted by law or regulation, Snowflake and Customer shall mutually agree in advance on the details of the CJIS Audit, including the reasonable start date, scope and duration of the work, fees (if any), how the work will be conducted (e.g., through interviews, document reviews, questionnaires), and shall mutually agree to the security and confidentiality controls that You or the authorized third party will implement to ensure adequate security. In no event will such CJIS Audits include direct physical access to systems, networks, or applications or access to other customers' data. The CJIS Audit must not violate, adversely impact, or otherwise effect Snowflake's contractual commitments to third parties.
3. Any expenses incurred by You in connection with any such CJIS Audit shall be borne exclusively by You.
4. Any information related to Snowflake, its affiliates or suppliers, or any of their services or technology arising from such CJIS Audit shall be considered Snowflake Confidential Information under the Use Terms and subject to the confidentiality terms therein.
5. You must retain and/or include markings on all Snowflake Offering information, including but not limited to markings related to attorney client privilege and proprietary and confidential information, including information provided as part of such CJIS Audit.
6. You must notify Reseller promptly, and not more than 48 hours after discovery, of any unauthorized disclosure of or access to Snowflake Confidential Information (including Snowflake proprietary information, sensitive business information, or personally identifiable information) provided to You in connection with such CJIS Audit.
7. You must delete all documents and other artifacts related to such CJIS Audit within one year, except that You may retain a copy of the final report for so long as needed to comply with legal requirements, after which You must delete all information in Your possession related to such CJIS Audit.

ii. You shall use reasonable commercial efforts to ensure the provisions set forth in Section 3(d)(i) will also apply to any CJIS Audits performed by third parties authorized under the CJIS Security Policy to perform such CJIS Audits.

iii. Notwithstanding the foregoing, You acknowledge that because Snowflake personnel may not have visibility to the content of Customer Data (and therefore any Customer Data that qualifies as CJI) in Your CJIS Covered Accounts, Snowflake, may not be able to provide information as to the particular nature of such Customer Data.

4. **Your Responsibilities.**

a. **Customer Assessment**. Notwithstanding any provision to the contrary herein, for CJIS Covered Accounts, You are responsible for (i) reviewing the Documentation and assessing and selecting the appropriate CJIS Region for the uploading, processing, storing, or transmitting of Customer Data that qualifies as CJI, as well as understanding the Service, including the Snowflake CJIS Service and CJIS Ancillary Services, and appropriately activating and configuring it to protect against unauthorized use and access to Customer Data that qualifies as CJI; and (ii) otherwise complying with the CJIS Security Policy and CJIS Security Addendum. You represent and warrant that Your CJIS Covered Accounts satisfy the requirements imposed on You with respect to Customer Data that qualifies as CJI. You may only upload CJI to the Snowflake CJIS Service.

b. **Security Boundary**. You represent and warrant that, other than as mutually agreed upon in connection with the CJIS Ancillary Services, You will not provide any CJI to Snowflake other than by uploading the CJI to a CJIS Covered Account as Customer Data.

c. **Support**. Any support for CJIS Covered Accounts provided by Snowflake that may require access to unencrypted Customer Data will be provided by persons who are lawfully permitted to access Customer Data that qualifies as CJI and in accordance with the Support Policy, provided that You submit support requests through a support ticket or You contact Snowflake support at +1-888-239-6019, and, in each case, indicate in such support request that You have a U.S. SnowGov Region Access Account.

d. **Personnel**.

i. If You desire to provide access to unencrypted CJI to Snowflake personnel that are not Covered Snowflake Personnel (which may only occur in connection with the CJIS Ancillary Services), You must provide advance, written notice and obtain written confirmation from Snowflake that such individuals have satisfied the requirements in Section 3(b) for Covered Snowflake Personnel before providing such personnel access to the CJI. Such individuals will be considered Covered Snowflake Personnel.

ii. If You elect to screen Snowflake personnel to satisfy Your own screening procedures or requirements:

1. You will inform Reseller in writing and Reseller will provide You with a list of all Covered Snowflake Personnel.
2. You are solely responsible for screening all Covered Snowflake Personnel, including obtaining all necessary consents; paying all charges, fees and other costs related to such screening; and ensuring that all Covered Snowflake Personnel have successfully completed Your screening requirements and the screening requirements set out in the CJIS Security Policy as applicable to CJI, prior to uploading Customer Data that qualifies as CJI to the Snowflake CJIS Service or procuring any CJIS Ancillary Services.
3. You must ensure that all such screening of Snowflake personnel, and related activities, are conducted in compliance with applicable law, including but not limited to the CJIS Security Policy and the Fair Credit Reporting Act (15 U.S.C § 1681 *et seq.*).
4. You shall provide Snowflake with written confirmation that Covered Snowflake Personnel have successfully completed Your screening requirements and the screening requirements set out in the CJIS Security Policy as applicable to CJI.
5. You shall: (a) provide the screening results to the applicable Snowflake personnel (or personnel applicants) upon request; and (b) provide the screening results to Snowflake, but only with the consent of the personnel (or personnel applicants) and only upon Snowflake's written request.
6. To the extent permitted under applicable laws, You shall indemnify and hold Snowflake harmless for any unauthorized access and/or use of Covered Snowflake Personnel information obtained by You in compliance with this Section 4(d)(ii) ("**Covered Snowflake Personnel Screening Information**"). Where You, in accordance with applicable laws, are prohibited from providing the aforementioned indemnity, You understand and agree that You are solely responsible for all risks and, notwithstanding any provision to the contrary hereunder or in the U.S. SnowGov Region Access Terms or Use Terms, all claims, liability, costs, damages, penalties arising from or relating to any Covered Snowflake Personnel Screening Information collected by You.
7. You hereby represent and warrant that You will not use or allow any third party to use such data other than as expressly required to comply with the CJIS Security Policy. The foregoing obligations shall not apply to unauthorized access and/or use of Covered Snowflake Personnel Screening Information to the extent caused by an act or omission of Snowflake.

e. **Government Communications**. Snowflake shall provide all communications required hereunder to You. You will comply with the third party communication requirements in the CJIS Security Policy, CJIS Security Addendum, and which are otherwise applicable to Customer Data that qualifies as CJI or CJIS Covered Accounts, including all notice and correspondence to third party government entities. For clarity, nothing hereunder requires Snowflake to communicate with any third party.

5. **Miscellaneous.**

a. **Term**. This CJIS Access Terms Addendum is effective as of the CJIS Access Terms Addendum Effective Date and will remain in effect for so long as You are using CJIS Covered Accounts, unless terminated earlier in accordance with the, the U.S. SnowGov Region Access Terms, the Use Terms or applicable law. This CJIS Access Terms Addendum, any access to the Snowflake CJIS Service or use of CJIS Ancillary Services, and/or the uploading, processing, storing, or transmitting of Customer Data that

qualifies as CJI may be immediately terminated if You cease to meet applicable eligibility requirements for any Snowflake CJIS Service or breach the terms of this CJIS Access Terms Addendum.

b. **Assignment**. Notwithstanding anything to the contrary in the U.S. SnowGov Region Access Terms or the Use Terms, You may not assign this CJIS Access Terms Addendum without advance written consent of Reseller.

c. **Confidentiality**. This CJIS Access Terms Addendum constitutes Snowflake Confidential Information under the Use Terms and is subject to the confidentiality terms therein.

d. **Severability; Interpretation**. If a court of competent jurisdiction holds any provision of this CJIS Access Terms Addendum to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this CJIS Access Terms Addendum will otherwise remain in effect. Section headings are inserted for convenience only and shall not affect the construction of this CJIS Access Terms Addendum.

e. **Entire Agreement; Conflict**. This CJIS Access Terms Addendum, together with the U.S. SnowGov Region Access Terms and the Use Terms, are the complete and exclusive statement of the mutual understanding of the parties and supersede and cancel all previous written and oral agreements and communications relating to the subject matter of this CJIS Access Terms Addendum. Except as specifically set forth in this CJIS Access Terms Addendum, all terms and conditions of the Use Terms and the U.S. SnowGov Region Access Terms remain in full force and effect. In the event of any conflict between this CJIS Access Terms Addendum, Use Terms and the U.S. SnowGov Region Access Terms, this CJIS Access Terms Addendum will control with respect to the subject matter herein.

Accepted and agreed to as of the CJIS Access Terms Addendum Effective Date by the authorized representative of each Party:

YOU	**RESELLER**
_____	_____
Signature	Signature
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____
Date	Date