THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

SAN BERNARDINO COUNTY

Contract Number
20-1028 A1

SAP Number

Innovation and Technology Department

Department Contract Representative	**Lea Radimaker**
Telephone Number	909-388-0672
Contractor	Amazon Web Services
Contractor Representative	**Kris Piper**
Telephone Number	**949-375-5537**
Contract Term	10/27/20 through 10/26/30
Original Contract Amount	Not-to-exceed $3,500,000
Amendment Amount	N/A
Total Contract Amount	Not-to-exceed $3,500,000
Cost Center	1200604048

Briefly describe the general nature of the contract: *Amendment to AWS Customer Agreement to accept AWS GovCloud (US) Addendum for Direct AWS Customers Last Updated: 1/20/2021 for AWS cloud services and storage.*

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
► Bonnie Uphold	►	►
Bonnie Uphold, Supervising Deputy County Counsel		
Date 3-1-2023	Date	Date

AWS GovCloud (US) Addendum for Direct AWS Customers

Last Updated: 1/20/2021

NOTE:

- You may click-through this AWS Govcloud (US) Addendum (**"GovCloud Addendum"**) to request access to the AWS GovCloud (US) regions (referred to as **"GovCloud Regions"**) **only if you are a direct** AWS customer (i.e., you have clicked-through the AWS customer agreement (aws.amazon.com/agreement) (as updated from time to time) or have entered into another agreement with AWS for the use of AWS Services (**"Agreement"**)). You may not click-through to request access to the GovCloud Regions if you acquire AWS Services through an AWS Solution Provider (**"Solution Provider"**).
- If you are not a direct AWS customer, please contact your Solution Provider for instructions on how to open an ccount to access the AWS GovCloud Regions.

The GovCloud Adddenum applies to your/Customers (**"your"** or **"you"**) use and access of the Service Offerings in the GovCloud Regions. The GovCloud Addendum supplements your Agreement with AWS. You represent to us that you are lawfully able to enter into contracts including this Addendum,and if you are entering into the GovCloud Addendum for an entity, such as the entity or company you work for, you represent to us that you have legal authority to bind that entity. The GovCloud Addendum takes effect the earlier of: (i) when you click an "I Accept" button or check box presented with the GovCloud Addendum; or (ii) when you access or use any of the AWS Services in the GovCloud Regions. Unless otherwise defined in the GovCloud Addendum, all capitalized terms will have the meanings ascribed to them in the Agreement.

1. **AWS Security.** AWS will implement reasonable and appropriate measures for AWS's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within AWS's control and are used to provide the Services in the GovCloud Regions (referred to as the **"AWS Network"**) in accordance with the GovCloudSecurity Standards (as defined in paragraph 2). The GovCloud Security Standards are designed to: (i) help you secure Your Content/Customer Content (**"Your Content"**) against accidental or unlawful loss, access, or disclosure; (ii) implement the in-scope Federal Risk and Authorization Management Program (**"FedRAMP"**) and Department of Defense Cloud Computing Security Requriements Guide (**"DoD SRG"**) controls for the Services identified as FedRamp compliant on the AWS Site (the **"Services in Scope"**), and (iii) maintain physical and logical access controls to limit access to the AWS Network by AWS personnel, including employees and contractors, to U.S. citizens, as defined by 8 U.S. Code §1401, et seq. (**"U.S. Citizens"**) ((i), (ii) and (iii) collectively the **"Security Objectives"**). During the term of the GovCloud Addendum, AWS will: (i) use commercially reasonable efforts to maintain FedRAMP and DoD SRG authorization at the then-current equivalent authorization for the then-current Services in Scope; and (ii) maintain an information security program designed to provide at least the same level of protection as evidenced by its FedRAMP and DoD SRG Authorizations to Operate (or its successor or equivalent, as reasonably determined by AWS) as of the Addendum Effective Date.

2. **GovCloud Security Standards.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to: satisfy the Security Objectives; identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network; and minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures: (i) **Network Security.** The AWS Network will be electronically accessible to employees, contractors, and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats; (ii) **Physical Security** (a) Physical components of the AWS Network are housed in nondescript facilities (the **"Facilities"**). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation or validation by human security personnel. Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities. (b) AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates. (c) All access

points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited; and (iii) **Continued Evaluation**. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

3. **Your Obligations.**

   a. **Representations and Warranties.** You represent and warrant that you: (i) are a U.S. Person, as defined by 22 CFR part 120.15 ("**U.S. Person**"); (ii) will only assign a U.S. Person as your account owner for your AWS GovCloud (US) account; (iii) are opening an account on behalf of an organization that is a U.S. entity; (iv) are not subject to U.S. export restrictions or sanctions, and are not suspended or debarred from contracting with any U.S. government entities u and (v) will, if required by the International Traffic in Arms Regulations ("ITAR"), have and maintain a valid Directorate of Defense Trade Controls registration and an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested by AWS, you agree to provide AWS with additional documentation and cooperation to verify the accuracy of the representations and warranties set forth in this Section.

   b. **Your Responsibilities.** You are responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, your account access, data transmission, encryption, and appropriate storage and processing of data within the GovCloud Regions. You are responsible for verifying that all End Users accessing Your Content in the GovCloud Regions are eligible to gain access to Your Content. The Services may not be used to process or store classified data. If you introduce classified data into the AWS Network, you will be responsible for all sanitization costs incurred by AWS or its Affiliates. Your liability under this provision is exempt from any limitations of liability.

4. **Termination of the Addendum.** This Addendum shall continue in force until the termination of the Agreement, unless terminated earlier by you or AWS in accordance with the Agreement.

5. **Nondisclosure.** Except as prohibited by law, you agree that the existence and details of the Addendum are not publicly known and will not be disclosed by you. If you are lawfully requested to disclose information about the Addendum, you agree to provide AWS with advance written notice and an opportunity to seek a protective order or other order that protects against disclosure of the Addendum unless such prior notice is prohibited by law.

6. **Entire Agreement; Conflict.** The Agreement will remain in full force and effect. The Addendum, together with the Agreement: (a) are intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersede all prior agreements and understandings between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement, the Addendum, or any other amendment or addendum to the Agreement or Addendum, the document later in time will prevail.

County of San Bernardino
DELEGATED AUTHORITY – DOCUMENT REVIEW FORM

This form is for use by any department or other entity that has been authorized by Board of Supervisors/Directors action to execute grant applications, awards, amendments or other agreements on their behalf. All documents to be executed under such delegated authority must be routed for County Counsel and County Administrative Office review prior to signature by designee.

Note: This process should NOT be used to execute documents under a master agreement or template, or for construction contract change orders. Contact your County Counsel for instructions related to review of these documents.

Complete and submit this form, along with required documents proposed for signature, via email to the department's County Counsel representative and Finance Analyst. If the documents proposed for signature are within the delegated authority, the department will submit the requisite hard copies for signature to the County Counsel representative. Once County Counsel has signed, the department will submit the signed documents in hard copy, as well as by email, to CAO Special Projects Team for review. If approved, the department will be provided routing instructions as well as direction to submit one set of the executed documents to the Clerk of the Board within 30 days.

For detailed instructions on submission requirements, reference Section 7.3 of the Board Agenda Item Guidelines as the Delegation of Authority does not eliminate the document submission requirements.

Department/Agency/Entity: **Innovation and Technology Department**

Contact Name: **Lea Radimaker** Telephone: **909-388-0672**

Agreement No.: **20-1028** Amendment No.: **1** Date of Board Item **10/27/20** Board Item No.: **52**

Name of Contract Entity/Project Name: **Amazon Web Services**

Explanation of request/Special Instructions:
ISee Attached

CLERK OF THE BOARD OF SUPERVISORS
2023 MAR -7 AM 9:54
COUNTY OF SAN BERNARDINO CALIFORNIA

Insert check mark that the following required documents are attached to this request:

☒ **Documents proposed for signature (Note: For contracts, include a signed non-standard contract coversheet for contracts not submitted on a standard contract form).**

☒ **Board Agenda item that delegated the authority**

Department Routed to County Counsel	County Counsel Name: Bonnie Uphold	Date Sent: 3/1/23
Reviewing County Counsel Use Only	Review Date 3-1-2023 Bonnie Uphold Signature	**Determination:** X Within Scope of Delegated Authority ___Outside Scope of Delegated Authority
CAO-Special Projects Use Only	Review Date 3/3/23 Signature	**Disposition:** ✓ Route for signature to: ___Chair ___CEO ✓ Department ___Return to Department for preparation of agenda item