

Appendix G to DIR Contract Number DIR-TSO-2733
AWS GovCloud

This Addendum No. 1 (this “**Addendum**”) to the AWS Customer Agreement (Appendix G to DIR Contract Number DIR-TSO-2733) (the “**Agreement**”) by and between Amazon Web Services, Inc. (“**AWS**”, “**we**”, “**us**” or “**our**”) and _____ [INSERT NAME OF ELIGIBLE DIR CUSTOMER] (“**you**” or “**Customer**”) is effective as of _____ [INSERT EFFECTIVE DATE] (the “**Addendum Effective Date**”). Unless otherwise defined in this Addendum, all capitalized terms used in this Addendum will have the meanings ascribed to them in the Agreement. The parties agree as follows:

1. **AWS Security.** Section 3.1 (“AWS Security”) of the Agreement is amended to add the following at the end of the section:

“Without limiting Section 10 or Customer’s obligations under Section 4, in accordance with the AWS Security Standards, for the AWS GovCloud(US) region AWS will implement reasonable and appropriate measures for the AWS Network designed to: (i) help Customer secure Customer Content against accidental or unlawful loss, access or disclosure; (ii) implement the in-scope Federal Risk and Authorization Management Program (“**FedRAMP**”) controls for the Services identified as FedRamp compliant; 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. persons, as defined by 22 CFR part 120.15 (“U.S. Persons”) ((i), (ii) and (iii) collectively the “Security Objectives”).”

2. **U.S. Persons Restricted Access.** The following Sections 3.1.1 and 3.1.2 are added to the Agreement:

3.1.1 U.S. Persons Restricted Access. The AWS GovCloud (US) region is the only AWS region that has physical and logical access controls that limit access to the AWS Network by AWS Personnel to U.S. Persons. You represent and warrant that you will only access the AWS GovCloud (US) region if: (i) you are a U.S. Person; (ii) you, if required by the International Traffic In Arms Regulations (“ITAR”), have and will maintain a valid Directorate of Defense Trade Controls registration; (iii) you are not subject to export restrictions under U.S. export control laws and regulations (e.g. you are not a denied or debarred party or otherwise subject to sanctions); and (iv) you maintain 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.

3.1.2 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 AWS GovCloud (US) region. You are responsible for verifying that all End Users accessing Your Content in the AWS GovCloud (US) region 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. Your liability under this provision is exempt from any limitations of liability.”

3. **Definitions.**

The definition of “End User” is deleted in its entirety and replaced with the following:



“‘End User’ means any entity, person, or United States Federal, State or Local Government agency that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account. The term “End User” does not include individuals or entities when they are accessing or using the Services or any Content under their own account, rather than your account.”

4. **Nondisclosure.** Subject to its legal obligations under the Texas Public Information Act, Texas Government Code Chapter 552, the parties will observe the confidentiality provisions of this agreement when issuing press releases or other public announcements, including this Addendum. If Customer receives a request under the Texas Public Information Act for the disclosure of Covered Information, including this Amendment, Customer will provide AWS with prior notice and a reasonable opportunity to prevent disclosure of the information.
5. **Entire Agreement; Conflict.** Except as amended by this Addendum, the Agreement will remain in full force and effect. This Addendum, together with the Agreement as amended by this Addendum: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. This document, DIR Contract Number DIR-TSO-2733 and its attachments and amendments make up the entire agreement.
6. **Counterparts and Facsimile Delivery.** This Amendment may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may sign and deliver this Amendment by facsimile transmission.

[Remainder of Page Intentionally Left Blank.]



IN WITNESS WHEREOF, Company and AWS have executed this Amendment as of the Amendment Effective Date.

AMAZON WEB SERVICES, INC.

[NAME OF ELIGIBLE DIR CUSTOMER]

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

