SCO ID:

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-14328	CDT-7502

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME

California Department of Technology

CONTRACTOR NAME

Rackspace US, Inc.

2. The term of this Agreement is:

START DATE

May 17, 2022

THROUGH END DATE

May 31, 2024

3. The maximum amount of this Agreement is:

$50,000,000.00 - Fifty Million and Zero Cents

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

	Exhibits	Title	Pages
	Exhibit A	Statement of Work	7
	Exhibit A-1	Service Level Agreements (SLAs)	1
	Exhibit B	Payment and Invoicing	2
+ -	Exhibit C	Cost Proposal Worksheet	1
+ -	Exhibit D	California Department of Technology Special Terms and Conditions to Safeguard Federal Tax Information	9
+ -	Exhibit E	FedRAMP Moderate Cloud Computing General Provisions - Information Technology	18
+ -	Exhibit F	FedRAMP Moderate Cloud Computing Special Provisions (Infrastructure as a Service and Platform as a Service)	6
+ -	Exhibit G	AWS Service Agreement	11
+ -	Exhibit H	AWS Security Standards	2
+ -	Exhibit I	Mutual Nondisclosure Agreement	3
+ -		Contractor's final proposal and the entire invitation to Negotiate, Event ID 0000019460, are hereby incorporated as part of this contract.	

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at https://www.dgs.ca.gov/OLS/Resources

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

CONTRACTOR

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)

Rackspace US, Inc.

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
1902 Campus Commons Drive, Suite 510	Reston	VA	20191

PRINTED NAME OF PERSON SIGNING	TITLE
Rick Rosenburg	VP & GM, Government Solutions

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
R. Rosenburg R. Rosenburg (May 17, 2022 16:45 EDT)	May 17, 2022

SCO ID:

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES
STANDARD AGREEMENT
STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-14328	CDT-7502

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME			
California Department of Technology			
CONTRACTING AGENCY ADDRESS	CITY	STATE	ZIP
10860 Gold Center Drive	Rancho Cordova	CA	95670
PRINTED NAME OF PERSON SIGNING	TITLE		
Russ Nichols	Acting Director		
CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED		
Russ Nichols (May 17, 2022 14:05 PDT)	May 17, 2022		
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)		
	Exempt per CDT Purchasing Authority Delegation No. CDT-7502		

EXHIBIT A
STATEMENT OF WORK

1. Contract Description

Rackspace US, Inc. (hereinafter referred to as the "Contractor") agrees to provide the State of California and local government agencies, via the California Department of Technology (CDT) (hereinafter referred to as the "State" and/or "CDT"), the entire portfolio of products as identified in the contract and will be the primary point of contact for data collection, reporting, and provisions of Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) Cloud Services for the Moderate level to the State. This Statement of Work (SOW) covers terms and conditions for the entire portfolio of products as identified in the contract for IaaS and/or PaaS.

Contractor is not allowed to offer any telecommunications or other services that are offered in the Amazon Web Services (AWS) Marketplace or portal where those, or like products or services conflict with other State mandatory contracts. Contractor shall work cooperatively with CDT to ensure prohibited Marketplace products are not resold through this Contract.

This includes cloud based voice services, traditional analog, digital, IP, and wireless telecommunications services. Cloud based voice services include but are not limited to Cloud Telephony, Cloud Calling, Cloud PBX , Contact Center, Unified Communications, Video Conferencing, or any other cloud based software or service that facilitates the transmission, management or operation of voice or other communications.

2. Term/Period of Performance

a. The term of this Agreement shall commence on May 17, 2022, or the date the Agreement is approved by the California Department of Technology, whichever is later (referred to herein as the "Effective Date") and continue through May 31, 2024.
b. The State reserves the option to extend the term of this Agreement at its sole discretion for up-to two (2) optional, two (2) year extensions.
c. The Contractor shall not be authorized to deliver or commence services as described in this SOW until written approval has been obtained from the State. Any delivery or performance of service that is commenced prior to the signing of the Agreement shall be considered voluntary on the part of the Contractor and not eligible for payment nor compensation.

3. Contractor's Proposal Response

The Contractor's response and Request for Proposal (RFP) Number 33526 are incorporated by reference into this Agreement as if attached hereto.

4. Installed On

The cloud IaaS and/or PaaS is wholly AWS-owned, managed and installed at the Cloud Service Provider (CSP) or the Contractor's site.

5. Data/Information Categorization:

Per SAM 5305.5, the State's data housed on the Contractor's server(s) must be at the FedRAMP Moderate level.

6. Notices

All notices required by, or relating to, this Agreement shall be in writing and shall be sent to the parties of this Agreement at their address as contained within unless changed from time to time, in which event each party shall notify the other in writing, and all such notices shall be deemed duly given if deposited, postage prepaid, in the United States mail or e-mailed and directed to the customer service contacts referenced in the User Instructions.

The technical representative during the term of this Agreement will be:

State Agency		Manufacturer	
CDT, Office Technology Services		Amazon	
Attn:	Scott MacDonald	Attn:	Mark Spitzer
Phone:	(916) 228-6460	Phone:	(916) 223-5373
E-mail:	Scott.Macdonald@state.ca.gov	Web:	spitzerm@amazon.com

Contract inquiries should be addressed to:

State Agency		Contractor	
CDT, Acquisitions & IT Program Management Branch		Rackspace US, Inc.	
Attn:	Jamie Wong	Attn:	Debbie Mckean
Address:	PO Box 1810 Rancho Cordova, CA 95741	Address:	1902 Campus Commons Drive, Suite 510 Reston, VA 20191
Phone:	(916) 857-9682	Phone:	(703) 732-8779
E-mail:	Jamie.Wong@state.ca.gov	E-mail:	Deborah.mckean@rackspace.com

7. Technical Requirements

a. The AWS GovCloud and AWS US East West Environments must be FedRAMP Authorized at the Moderate level (commensurate with the Program level being proposed by the proposal due date as identified in Section I.E., Key Action Dates).
b. The Contractor must provide a portal and training for CDT for self-provisioning. The training shall be included in the bid price.
c. The CSP must ensure, if using Network Edge Services, that the NIST ISO/IEC 27018:2019 certification has been achieved for the specific services being added to the portfolio. These services augment the AWS' IaaS and/or PaaS portfolio and may be included as part of the portfolio services without obtaining a FedRAMP Authorization to Operate (ATO) for that service. The Network Edge Services must have achieved NIST ISO/IEC 27018:2019 certification, which provides guidance aimed at ensuring that CSP's offer suitable information security controls to protect the privacy of their customers' clients by securing Personally Identifiable Information (PII) entrusted to them, for the specific service being added to the portfolio. Services that have the potential of containing confidential and/or sensitive data must have the ability to contain that service within the continental United States.
d. The CSP shall enable the State to encrypt Personal Data and Non-Public Data at rest, in use, and in transit with controlled access. The SOW and/or Service Level Agreement (SLA) will specify which party is responsible for encryption and access control of the State Data for the service model under the Agreement. If the SOW and/or SLA and the Agreement are silent, then the State is responsible for encryption and access control.

e. The CSP must provide the state with the root access to the master payer account.

Application Programming Interface Requirements (M)

AWS' IaaS and/or PaaS must provide open Application Programming Interfaces (API) that provide the capability to:

a. Migrate workloads between the public cloud and the State's private on-premise cloud where CDT acts as the broker of those services and has the ability to logically separate individual customers;
b. Define networks, resources and templates within a multi-tenant environment with the use of available APIs;
c. Provision and de-provision virtual machines and storage within a multi-tenant environment;
d. Add, remove and modify computing resources for virtual machines within a multi-tenant environment;
e. Add, remove and modify object and block storage within a multi-tenant environment;
f. Retrieve financial and billing information that provides detailed information for each CDT customer (i.e. Eligible Public Entity) subscriber;
g. Retrieve performance indicators for all workloads in the multi-tenant environment;
h. Retain all workloads and support within the U.S.
i. Retrieve log data from all workloads; and
j. Provide the ability to model potential workloads to determine cost of services.

Environment Requirements (M)

The AWS IaaS/PaaS cloud environment must have the ability to:

a. Provide a multi-tenant environment that supports a parent/child administrative relationship that enables the CDT (parent) to programmatically apply compliance and regulatory requirements and standards down to the Eligible Public Entities.
b. Provide all tested and compliant modules under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search **and/or** with FIPS 140-3 compliant cryptographic modules https://csrc.nist.gov/publications/detail/fips/140/3/final;
c. Support cost tracking by resource tags or other solutions to tracking costs for Eligible Public Entities;
d. Run and manage web applications, including .NET environments;
e. Provide managed database services with support for multiple database platforms;
f. Support Security Access Markup Language (SAML) federation;
g. Provide integration with a customer's on premise Active Directory;
h. Provide a managed service to create and control encryption keys used to encrypt data;
i. Provide a dedicated Hardware Security Module (HSM) appliance for encryption key management;
j. Provide services to migrate workloads to and from the State's VMware and HyperV environments; and
k. Provide dashboard reporting that provides performance monitoring, usage and billing information.

8. Reserved Instances (NM)

Reserved Instances may be available for use on this Agreement.

9. Contractor Responsibilities

a. The Contractor will assign a contact person for contract management purposes. The Contractor Contract Manager must be authorized to make decisions on behalf of the Contractor.
b. The Contractor shall allow the CDT or its designated third party to audit conformance including but not limited to contract terms, pricing, costing, ordering, invoicing, and reporting. Such reviews shall be conducted with at least thirty (30) calendar days advance written notice and shall not unreasonably interfere with the Contractor's business. The CSP shall allow the CDT or its designated third party to audit conformance to Attachment 14.B.4, Application Programming Interface, and Attachment 14.B.5, Environment.
c. The Contractor shall promptly notify the Eligible Public Entity in writing of any unresolved issues or problems that have been outstanding for more than three (3) business days. The Eligible Public Entity shall notify the Contractor of the same.
d. The Contractor will ensure all promotional materials or press releases referencing the contract shall be submitted to the CDT Contract Administrator for review and approval prior to release.
e. The Contractor shall only accept orders from CDT. The Contractor shall not accept purchase documents for this contract that: are incomplete; contain non-contract items; or contain non-contract terms and conditions. The Contractor must not refuse to accept orders from CDT for any other reason without written authorization from the CDT Contract Administrator.
f. The Contractor must provide CDT with an order receipt acknowledgment via e-mail within one (1) business day after receipt of an order.
g. The Contractor shall ensure invoices be submitted to the CDT on behalf of the Eligible Public Entity on a quarterly or monthly basis in arrears.

   Invoices must include:
   - Eligible Public Entity Name
   - Dollar amounts
   - Usage
   - Discount
   - Date of provided services
   - Purchase Order number
   - Item Description
   - Booking Confirmation #
   - Product name
   - Code/description/customer department/subscription account number (if applicable)
   - Term date

h. The Contractor will ensure payments are to be made in accordance with Sections 23 of Exhibit E – FedRAMP Moderate Cloud Computing General Provisions – Cloud Computing.
i. The Contractor must provide the State with a catalog of authorized services and architecture patterns.
j. The Contractor must maintain an online catalog of available SLAs meeting the minimum requirements of Section VI, Business/Technical Requirements.

1) The catalog website shall contain:
   i. Detailed descriptions of available IaaS and/or PaaS Cloud Services SLAs; and
   ii. Public pricing (MSRP/MSLP) on which the State discount is based.

2) The Contractor shall notify the State of any updates to the Catalog website.

10. State's Responsibilities

a. CDT will be the only authorized user of the contract and will submit orders on behalf of Eligible Public Entities using a Purchasing Authority Purchase Order (Std. 65) or using the FI$Cal Purchase Order process. Blanket orders are acceptable.
b. The State reserves the right to receive credits in the event the Contractor fails to meet an applicable SLA (see Exhibit A-1).

11. Information and Data Ownership

All information and data stored by the State of California (this includes all public agencies in the State of California that may use this Agreement) using the service provider's system(s) remains the property of the State. As such, the service provider agrees to not scan, capture or view such information or data unless expressly authorized by the appropriate representatives of the State of California. Prior to the release of any information or data belonging to the State of California to any law enforcement agency, the service provider must notify and gain the express approval of the CDT and the California Department of Justice. The service provider may respond to subpoenas or other judicial mandates that forbid notice to CDT, without breach of contract. Upon the conclusion of service as notified by the State, the service provider must provide to the State a copy of all State data stored in the service providers system within five (5) business days in the Exit Data Format specified in the technical requirements. The State and the Contractor may mutually agree on a longer time period, as required by the amount of data or the format requested. Upon acceptance of this data by the State of California, the service provider shall purge the data from any and all of its systems and provide the State confirmation that such steps have occurred within ten (10) business days. Failure to comply with any of these terms may be grounds for termination for default.

12. Problem Escalation

a. The parties acknowledge/agree that certain technical and project-related problems or issues may arise and that each party shall bring such matters to the immediate attention of the other party when identified. Known problems or issues shall be reported in regular weekly status reports or meetings. However, there may be instances where the severity of the problem justifies escalated reporting. To this extent, the State will determine the next level of severity, and notify the appropriate State and CSP personnel. The personnel notified, and the time-period taken to report the problem or issue, shall be at a level commensurate with the severity of the problem or issue.

b. The State personnel include, but are not limited to the following:

First Level: Service Desk – (916) 464-4311, ServiceDesk@state.ca.gov
Second Level: Christine Nguyen – (916) 228-6414, Christine.Nguyen@state.ca.gov or Taron Walton – (916) 228-6317, Taron.Walton@state.ca.gov
Third Level: Cary Yee, (916) 228-6493, Cary.Yee@state.ca.gov
Fourth Level: Scott MacDonald – (916) 228-6460, Scott.Macdonald@state.ca.gov

c. The Contractor personnel include, but are not limited to the following:

First Level: Kevin Hamilton, (551) 655 - 3264, Kevin.Hamilton@rackspace.com
Second Level: Beth Scheidt, (410) 279 - 1236, Beth.Scheidt@rackspace.com
Third Level: Rick Rosenburg, (703) 909 - 9246, Rick.Rosenburg@rackspace.com

13. Amendments

Consistent with the terms and conditions of the original solicitation, and upon mutual consent, CDT and the Contractor may execute amendments to this Agreement. No amendment or variation of the terms of this Agreement shall be valid unless made in writing, and agreed upon by both parties and approved by the State, as required. No verbal understanding or agreement not incorporated into the Agreement is binding on any of the parties. Changes to the contract regarding the administrator, list pricing and technical changes to SKUs and descriptions, will be handled by supplement only and must be approved by the contract administrator.

14. Cancellation Provisions

CDT may exercise its option to terminate the resulting Agreement at any time with thirty (30) calendar days' prior written notice.

15. Federal Tax Administration Requirements

Subject to the Internal Revenue Service (IRS), federal tax information (FTI) requirements, if an unfavorable response is received by the IRS, this contract will be terminated immediately, per Exhibit E – FedRAMP Moderate Cloud Computing General Provisions – Cloud Computing, Section 17, Termination for Default.

16. Security and Data Protection Requirements

The State must ensure Agreements with State and non-state entities include provisions which protect and minimize risk to the State when engaging in the development, use, or maintenance of information systems, products, solutions, or services.

17. DVBE Reporting

Military and Veteran Code (MVC) 999.5(d), Government Code (GC) 14841, and California Code of Regulations (CCR) 1896.78(e) require that if the Prime Contractor had a Disabled Veteran Business Enterprise (DVBE) firm perform any element of work in the performance of the Agreement, to report the DVBE information.

Prime Contractors are required to maintain records supporting the information that all payments to DVBE subcontractor(s) were made. The Prime DVBE Subcontracting form can be found at the following link: https://www.dgs.ca.gov/PD/Services/Page-Content/Procurement-Division-Services-List-Folder/File-a-DVBE-Subcontractor and the instructions can be found at the following link: http://www.documents.dgs.ca.gov/pd/smallbus/Prime%20DVBE%20Sub%20Report%20Instruction.doc. Completed forms are to be e-mailed to: primeDVBE@state.ca.gov.

18. Clarifications and Revisions to General and Special Provisions

AWS Seller Direct General Provisions – Cloud Computing Moderate shall be modified as follows:

1. Section 1 (Definitions): "Documentation" shall be modified as follows: "shall mean the user guides and admin guides for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time."

19. Reserved Instances

Reserved Instances (RIs) are available for use on this contract.

EXHIBIT A-1
SERVICE LEVEL AGREEMENTS (SLAs)

Upon award, the Contractor's SLA will be incorporated into the Agreement.

a) Service Credits

1) The State reserves the right to obtain credit in the event the Contractor fails to meet an applicable SLA.

2) Service Credits will be applied against State's next invoice. A Service Credit will be applicable and issued only if the credit amount is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other Contractor's service or account. The State's remedy for any non-excluded down time is the receipt of a service credit (if eligible) in accordance with the terms of this Exhibit A-1. Upon expiration or non-renewal of this Agreement, all service credits will be forfeited (for example, if the non-excluded downtime occurs in the last month of the Agreement term and State does not renew, then the service credit is forfeited).

b) Performance Discounts

1) In addition to any Service Credits described herein, in the event the Contractor fails to meet the Service Commitment for a period of three (3) consecutive months or an aggregate of five (5) months over an eighteen (18) month period, the State shall be entitled to an additional 15% discount off the next invoice following month in which the Contractor failed to meet the Service Commitment.

Notwithstanding the Service Credits and Performance Discounts provided herein, the State reserves the right to terminate the contract pursuant to Section 17 of Exhibit E - FedRAMP Moderate Cloud Computing General Provisions – Information Technology, for Contractor's failure to meet the Service Commitment.

EXHIBIT B
PAYMENT AND INVOICING

1. Payment/Invoicing:

a. Payment for IaaS and/or PaaS will be made quarterly or monthly in arrears upon receipt of a correct invoice, except Reserved Instances (RIs) as described below. The invoice shall include booking confirmation of the CDT order; including but not limited to, the product name, code/description/customer department/subscription account number (if applicable), and term date, date of provided services; and shall reference the Agency Order Number.

1) Reserved Instances (RI) Payment/Invoicing

- Payment will be made according to the terms in this section, upon receipt of a correct invoice for RI(s) and must be included separately as its own line item and identified as an RI.

b. Fiscal Management Report

1) The Contractor agrees to provide quarterly Fiscal Management Reports electronically in Excel format, as shown in Item 3) Sample Template below, identifying services in accordance with the Agreement at no additional cost. The report must contain, but not limited to, the product name, code/description/customer department/subscription account number, term date, services being utilized, and the monthly amount being charged.

2) Adhoc reports must be provided when/if requested.

3) Sample Template

Account Name	Account Number	Month 1 Charges	Month 2 Charges	Month 3 Charges	TOTAL
Department Name	000000000	100.00	100.00	100.00	300.00

c. Submit your invoice using only **one** of the following options:

1) Send via U.S. mail in **TRIPLICATE** to:

California Department of Technology
Administration Division – Accounting Office
P. O. Box 1810
Rancho Cordova, CA 95741

OR

2) Submit electronically at: APInvoices@state.ca.gov.

2. Prompt Payment Clause:

Payment will be made in accordance with, and within the time specified, in Government Code Chapter 4.5, commencing with Section 927. Payment to small/micro businesses shall be made in accordance with and within the time specified in Chapter 4.5, Government Code 927 et seq.

3. Budget Contingency Clause:

a. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Contract does not appropriate sufficient funds for the program, this Contract shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor or to furnish any other considerations under this Contract and Contractor shall not be obligated to perform any provisions of this Contract.

b. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Contract with no liability occurring to the State, or offer a contract amendment to the Contractor to reflect the reduced amount.

EXHIBIT C
COST PROPOSAL WORKSHEET

Published list price or greater for IaaS offerings for FedRAMP Moderate.

Contract Line Item # (CLIN)	Item Description	Contract Discount
2	Infrastructure as a Service for FedRAMP Moderate	15.00%

Item Description	Reserved Instance Discount % off MSIP/MSRP
Infrastructure as a Service	***15.00%***

Published list price or greater for PaaS offerings for FedRAMP Moderate.

Item Description	Published List Price	Discount Level	Contract Discount %	Contract $
Platform as a Service	$250,000	Base	15%	$212,500.00
	$250,000	A	15%	$212,500.00
	$250,000	B	15%	$212,500.00
	$250,000	C	15%	$212,500.00
	$1,000,000		**Evaluated Total:**	$850,000.00

Item Description	Reserved Instance Discount % off MSIP/MSRP
Platform as a Service	***15.00%***

(link to catalog)	https://calculator.aws/#/

EXHIBIT D
CALIFORNIA DEPARTMENT OF TECHNOLOGY SPECIAL TERMS AND CONDITIONS TO SAFEGUARD FEDERAL TAX INFORMATION

Federal statute, regulations and guidelines require that all contracts for services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes include the provisions contained in this exhibit. (See 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1(a)(2) and (d); Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (Rev. 9-2016), Section 5.5 and Exhibit 7.)

The contractor agrees to comply with 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1; IRS Publication 1075 (Rev. 9-2016); and all applicable conditions and restrictions as may be prescribed by the IRS by regulation, published rules or procedures, or written communication to the contractor. (See 26 C.F.R. §301.6103(n)-1(d); IRS Publication 1075 (Rev. 9-2016))

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. 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 or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined 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 Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized 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. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material 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 the contract. Inspection by or disclosure to anyone without an official need to know 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.

Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(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 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 individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training 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 both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a

confidentiality statement certifying their understanding of the security requirements.[1]

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

REFERENCES

26 U.S.C. §6103(n)

Pursuant to regulations prescribed by the Secretary, returns and return information may be disclosed to any person, including any person described in section 7513 (a), to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration.

(1) 26 C.F.R. §301.6103(n)-1 Disclosure of returns and return information in connection with procurement of property and services for tax administration purposes.

(a) *General rule.* Pursuant to the provisions of section 6103(n) of the Internal Revenue Code and subject to the requirements of paragraphs (b), (c), and (d) of this section, officers or employees of the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, are authorized to disclose returns and return information (as defined in section 6103(b)) to any person (including, in the case of the Treasury Department, any person described in section 7513(a)), or to an officer or employee of such person, to the extent necessary in connection with contractual procurement of—

(1) Equipment or other property, or

(2) Services relating to the processing, storage, transmission, or reproduction of such returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for purposes of tax administration (as defined in section 6103(b)(4)).

No person, or officer or employee of such person, to whom a return or return information is disclosed by an officer or employee of the Treasury Department, the State tax agency, the Social Security Administration, or the Department of Justice, under the authority of this paragraph shall in turn disclose such return or return information for any purpose other than as described in this paragraph, and no such further disclosure for any such described purpose shall be made by such person, officer, or employee to anyone, other than another officer or employee of such person whose duties or responsibilities require such disclosure for a purpose described in this paragraph, without written approval by the Internal Revenue Service.

(b) *Limitations.* For purposes of paragraph (a) of this section, disclosure of returns or return information in connection with contractual procurement of property or services described in such paragraph will be treated as necessary only if such procurement or the performance of such services cannot otherwise be reasonably, properly, or economically carried out or performed without such disclosure.

Thus, for example, disclosures of returns or return information to employees of a contractor for purposes of programming, maintaining, repairing, or testing computer equipment used by the Internal Revenue Service or a State tax agency should be made only if such services cannot be reasonably, properly, or economically performed by use of information or other data in a form which does not identify a particular taxpayer. If, however, disclosure of returns or return information is in fact necessary in order for such employees to reasonably, properly, or economically perform the computer related

[1] A 30 minute disclosure awareness training video produced by the IRS can be found at http://www.irsvideos.gov/Governments/Safeguards/DisclosureAwarenessTrainingPub4711

services, such disclosures should be restricted to returns or return information selected or appearing at random. Further, for purposes of paragraph (a), disclosure of returns or return information in connection with the contractual procurement of property or services described in such paragraph should be made only to the extent necessary to reasonably, properly, or economically conduct such procurement activity. Thus, for example, if an activity described in paragraph (a) can be reasonably, properly, and economically conducted by disclosure of only parts or portions of a return or if deletion of taxpayer identity information (as defined in section 6103(b)(6) of the Code) reflected on a return would not seriously impair the ability of the contractor or his officers or employees to conduct the activity, then only such parts or portions of the return, or only the return with taxpayer identity information deleted, should be disclosed.

(c) *Notification requirements.* Persons to whom returns or return information is or may be disclosed as authorized by paragraph (a) of this section shall provide written notice to their officers or employees—

(1) That returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized by paragraph (a) of this section;

(2) That further inspection of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a 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 costs of prosecution;

(3) That further disclosure of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section 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;

(4) That any such unauthorized further inspection or disclosure of returns or return information may also result in an award of civil damages against any person who is not an officer or employee of the United States in an amount not less than $1,000 for each act of unauthorized inspection or disclosure or the sum of actual damages sustained by the plaintiff as a result of such unauthorized disclosure or inspection as well as an award of costs and reasonable attorney's fees; and

(5) If such person is an officer or employee of the United States, a conviction for an offense referenced in paragraph (c)(2) or (c)(3) of this section shall result in dismissal from office or discharge from employment.

(d) *Safeguards.* Any person to whom a return or return information is disclosed as authorized by paragraph (a) of this section shall comply with all applicable conditions and requirements which may be prescribed by the Internal Revenue Service for the purposes of protecting the confidentiality of returns and return information and preventing disclosures of returns or return information in a manner unauthorized by paragraph (a). The terms of any contract between the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, and a person pursuant to which a return or return information is or may be disclosed for a purpose described in paragraph (a) shall provide, or shall be amended to provide, that such person, and officers and employees of the person, shall comply with all such applicable conditions and restrictions as may be prescribed by the Service by regulation, published rules or procedures, or written communication to such person. If the Service determines that any person, or an officer or employee of any such person, to whom returns or return information has been disclosed as provided in paragraph (a) has failed to, or does not, satisfy such prescribed conditions or requirements, the Service may take such actions as are deemed necessary to ensure that such conditions or requirements are or will be satisfied, including—

(1) Suspension or termination of any duty or obligation arising under a contract with the Treasury Department referred to in this paragraph or suspension of disclosures by the Treasury Department

otherwise authorized by paragraph (a) of this section, or

(2) Suspension of further disclosures of returns or return information by the Service to the State tax agency, or to the Department of Justice, until the Service determines that such conditions and requirements have been or will be satisfied.

(e) *Definitions.* For purposes of this section—

(1) The term *Treasury Department* includes the Internal Revenue Service and the Office of the Chief Counsel for the Internal Revenue Service;

(2) The term *State tax agency* means an agency, body, or commission described in section 6103(d) of the Code; and

(3) The term *Department of Justice* includes offices of the United States Attorneys.

IRS Publication 1075 (Rev. 9-2016**) Section *5.5 Control over Processing***

Processing of FTI, in an electronic media format, including removable media, microfilms, photo impressions, or other formats (including tape reformatting or reproduction or conversion to punch cards, digital images or hard copy printout) will be performed pursuant to one of the following procedures:

5.5.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.5.2 Contractor or Agency Shared Facility – Consolidated Data Centers

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.

Note: For purposes of applying sections 6103(l), (m) and (n), the term “agent” includes contractors. Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center.

The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 6103(n).

The contractor or agency-shared computer facility is also subject to IRS safeguard reviews.

Note: The above rules also apply to releasing electronic media to a private contractor or other agency office even if the purpose is merely to erase the old media for reuse.

Agencies utilizing consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA should cover the following:

1. The consolidated data center is considered to be a “contractor” of the agency receiving FTI. The agency receiving FTI – whether it is a state revenue, workforce, child support enforcement or human services agency – is responsible for ensuring the protection of all FTI received. However, as the “contractor” for the agency receiving FTI, the consolidated data center shares responsibility for safeguarding FTI as well.

2. Provide written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all federal tax information within their possession or control. The SLA should also include

details concerning the consolidated data center's responsibilities during a safeguard review and support required to resolve identified findings.

3. The agency will conduct an internal inspection of the consolidated data center every eighteen months (see section 6.3). Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care should be taken to ensure agency representatives do not gain unauthorized access to other agency's FTI during the internal inspection.

4. The employees from the consolidated data center with access to FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the consolidated data center that has access to FTI.

5. The specific data breach incident reporting procedures for all consolidated data center employees and contractors. The required disclosure awareness training must include a review of these procedures.

6. The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.

7. Identify responsibilities for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

Note: Generally, consolidated data centers are either operated by a separate state agency (example: Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision-making or implementation planning process. The purpose of these discussions is to ensure the agency remains in compliance with safeguarding requirements during the transition to the consolidated data center.

26 U.S.C. §7213. Unauthorized disclosure of information

(a) Returns and return information

(1) Federal employees and other persons

It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i)(3)(B)(i) or (7)(A)(ii), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), or (20) or (m)(2), (4), (5), (6), or (7) of section 6103.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(3) Other persons

It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(4) Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(5) Shareholders

It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution

(b) Disclosure of operations of manufacturer or producer

Any officer or employee of the United States who divulges or makes known in any manner whatever not provided by law to any person the operations, style of work, or apparatus of any manufacturer or producer visited by him in the discharge of his official duties shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution; and the offender shall be dismissed from office or discharged from employment.

(c) Disclosures by certain delegates of Secretary

All provisions of law relating to the disclosure of information, and all provisions of law relating to penalties for unauthorized disclosure of information, which are applicable in respect of any function under this title when performed by an officer or employee of the Treasury Department are likewise applicable in respect of such function when performed by any person who is a "delegate" within the meaning of section 7701(a)(12)(B).

(d) Disclosure of software

Any person who willfully divulges or makes known software (as defined in section 7612(d)(1)) to any person in violation of section 7612 shall be guilty of a felony and, upon conviction thereof, shall be fined not more than $5,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.

(e) Cross references

(1) Penalties for disclosure of information by preparers of returns

For penalty for disclosure or use of information by preparers of returns, see section 7216.

(2) Penalties for disclosure of confidential information

For penalties for disclosure of confidential information by any officer or employee of the United States or any department or agency thereof, see 18 U.S.C. 1905.

26 U.S.C. §7213A. Unauthorized inspection of returns or return information

(a) Prohibitions

(1) Federal employees and other persons
It shall be unlawful for—

(A) any officer or employee of the United States, or

(B) any person described in subsection (l)(18) or (n) of section 6103 or an officer or employee of any such person,
willfully to inspect, except as authorized in this title, any return or return information.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to inspect, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213 (a)(2) or under section 6104 (c).

(b) Penalty

(1) In general

Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) Federal officers or employees
An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) Definitions
For purposes of this section, the terms “inspect”, “return”, and “return information” have the respective meanings given such terms by section 6103 (b).

26 U.S.C. §7431. Civil damages for unauthorized inspection or disclosure of returns and return information

(a) In general

(1) Inspection or disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from a good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of -

(1) the greater of -

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of -

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the costs of the action, plus

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(d) Period for bringing action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of unlawful inspection and disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of -

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or

(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return", and "return information" have the respective meanings given such terms by section 6103(b).

1/17/2018

(g) Extension to information obtained under section 3406

For purposes of this section -

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103. For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

(h) Special rule for information obtained under section 6103(k)(9)

For purposes of this section, any reference to section 6103 shall be treated as including a reference to section 6311 (e).

EXHIBIT E
FEDRAMP MODERATE CLOUD COMPUTING GENERAL PROVISIONS-INFORMATION TECHNOLOGY

These FedRAMP Moderate Cloud Computing General Provisions - Information Technology ("FedRAMP Mod General Provisions") shall apply to all Eligible Public Entities' use of permitted Services, and are hereby added to the Contract.

---

1. DEFINITIONS:

Unless otherwise specified in the Statement of Work, the following terms shall be given the meaningshown, unless context requires otherwise.

a) **"Application Program"** means a computer program which is intended to be executed for the purpose of performing useful work for the user of the information being processed. Application programs are developed or otherwise acquired by the user of the Hardware/Software system, but they may be supplied by the Contractor.

b) **"Business entity"** means any individual, business, partnership, joint venture, corporation, S- corporation, limited liability company, sole proprietorship, joint stock company, consortium, or other private legal entity recognized by statute.

c) **"Buyer"** means the State's authorized contracting official.

d) **"Cloud Service Provider" (or "CSP")** means the service provider with FedRAMP Moderate authorization providing either IaaS or PaaS solicited through the IFB.

e) **"Contract"** means this Contract or agreement (including any purchase order), by whatever name known or in whatever format used.

f) **" Contractor"** means the Business Entity with whom the State enters into this Contract. Contractor shall be synonymous with "supplier", "vendor", "Reseller", or other similar term.

g) **"Customer"** means the Eligible Public Entity or the Users of the Contractor's or the CSP'sServices.

h) **"Deliverables"** means the Products and Services and other items (e.g. reports) to be delivered pursuant to this Contract, including any such items furnished that are incidental to the provision of services.

i) **"Documentation"** means the user guides and admin guides for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time.

j) **"Eligible Public Entity"** means each of the California public entities authorized to purchase the Deliverables and services offered hereunder which will be documented at the time of contract execution, and which the parties agree may be amended as needed from time to time. Eligible Public Entities shall be the "Customers" of the Contractor under applicable service agreements. "Eligible Public Entity" includes the State, county, city, city and county, district, public authority, public agency, municipal corporation, or any other political subdivision or public corporation in thestate, "Eligible Public Entity" also includes a federally-recognized tribal entity acting in its tribal governmental capacity.

k) **"FedRAMP"** is the Federal Risk and Authorization Management Program, or FedRAMP, which is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and

services.

l) **"FedRAMP Moderate"** is the framework for FedRAMP and uses the 800-53 security controls as published by NIST. The FedRAMP security controls are a baseline of controls designed to meet the needs of agencies using clouds systems at the low and moderate impact levels, but agencies can implement additional security controls for agency specific needs.

m) **"Goods"** means all types of tangible personal property, including but not limited to materials, supplies, and equipment (including computer and telecommunications equipment).

n) **"Hardware"** usually refers to computer equipment and is contrasted with Software. See also equipment.

o) **"Information Technology"** includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications which include voice, video, and data communications, requisite system controls, simulation, electronic commerce, and all related interaction between people and machines.

p) **"Infrastructure as a Service" (or "IaaS")** means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 or its successors.

q) **"Maintenance"** means that maintenance performed by the Contractor which results from a Services failure, and which is performed as required, i.e., on an unscheduled basis.

r) **"Platform as a Service" (or "PaaS")** means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 or its successors.

s) **"Product"** means any service offering solicited through this IFB and being made available through CDT for purchase by Eligible Public Entities.

t) **"Reseller"** means the agent(s) of the CSP authorized to perform aspects of this Agreement as specified herein including, but not limited to sales, fulfillment, invoicing, returns, and customer service.

u) **"Service Provider"** means the Contractor and includes the subcontractors, agents, resellers, third parties and affiliates of the Contractor who may provide the Services agreed to under the contract.

v) **"Services"** means the cloud computing services, including Infrastructure as a Service and Platform as a Service (but not Software as a Service), and any related services, offered to the State by the Contractor herein.

w) **"Software"** means an all-inclusive term which refers to any computer programs, routines, or subroutines supplied by the Contractor, including operating Software and Application Programs

x) **"State"** means the government of the State of California, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the State of California.

y) "State Data" means all data submitted to, processed by, or stored in the Service Provider's Services under this contract and includes but is not limited to all data that originated with the State, Eligible Public Entities, or Users, all data provided by

the State, Eligible Public Entities or Users, and data generated, manipulated, produced, reported by or otherwise emanating from or by applications run by the State or Users on the Services. For clarity, State Data is synonymous with "Customer Data" or "Customer Content" , as that term is used in various provisions of the service agreements and incorporated into the Contract and includes the following:

i. "Non-Public Data" means data submitted to the Service Provider's IaaS or PaaS Service, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that may be exempt by statute, regulation or policy from access by the general public as public information.

ii. "Personal Data" means data submitted to the Service Provider's IaaS or PaaS Service that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; Education Records; Employment Records; or protected health information (PHI) relating to a person.

a. "Education Records" covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

b. "Employment Records" held by a covered entity in its role as employer.

c. "Protected Health Information" (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes Education Records and Employment Records.

1) "Individually Identifiable Health Information" means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or
(b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

iii. "Public Data" means all other data not specifically mentioned above.

z) **"Statement of Work" (or "SOW")** means a document which defines a timeline, and specifies the objectives, deliverables or tasks for a particular project or service contract that outlines specific services a supplier is expected to perform, their responsibilities and expectations, indicating the type, level and quality of service that is expected, all of which form a contractual obligation upon the vendor in providing services to the client. The SOW includes detailed technical requirements and pricing, with standard regulatory and governance terms and conditions for cloud computing services, including Infrastructure as a Service and Platform as a Service but not Software as a Service, offered to the State by the Contractor herein.

aa) **"User" (see also "Customer")** means any end user, of the IaaS or PaaS services provided by the CSP under this Contract and includes Eligible Public Entities' employees, contractor's subcontractors, customers or any system utilized by the Eligible Public Entities to access the IaaS or PaaS services.

bb) **"U.S. Intellectual Property Rights"** means intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, copyrights, and U.S. patents.

2. CONTRACT FORMATION:

a) If this Contract results from a sealed bid offered in response to a solicitation conducted pursuant to Chapters 2 (commencing with Section 10290), 3 (commencing with Section 12100), and 3.6 (commencing with Section 12125) of Part 2 of Division 2 of the Public Contract Code (PCC), then Contractor's bid is a firm offer to the State which is accepted by the issuance of this Contract and no further action is required by either party.

b) If this Contract results from a solicitation other than described in paragraph a), above, the Contractor's quotation or proposal is deemed a firm offer and this Contract document is the State's acceptance of that offer.

c) If this Contract resulted from a joint bid, it shall be deemed one indivisible Contract. Each such joint Contractor will be jointly and severally liable for the performance of the entire Contract. The State assumes no responsibility or obligation for the division of orders or purchases among joint Contractors.

3. COMPLETE INTEGRATION:

This Contract, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of the Contract.

4. SEVERABILITY:

The Contractor and the State agree that if any provision of this Contract is found to be illegal or unenforceable, such term or provision shall be deemed stricken and the remainder of the Contract shall remain in full force and effect. Either party having knowledge of such term or provision shall promptly inform the other of the presumed non-applicability of such provision.

5. INDEPENDENT CONTRACTOR:

Contractor and the agents and employees of the Contractor, in the performance of this Contract, shall act in an independent capacity and not as officers or employees or agents of the State.

6. APPLICABLE LAW:

This Contract shall be governed by and shall be interpreted in accordance with the laws of the State of California; venue of any action brought with regard to this Contract shall be in Sacramento County, Sacramento, California. The United Nations

Convention on Contracts for the International Sale of Goods shall not apply to this Contract.

7. COMPLIANCE WITH STATUTES AND REGULATIONS

a) The State and the Contractor warrants and certifies that in the performance of this Contract, it will comply with all statutes and regulations of the United States and the State of California. For clarity, the Contractor will comply with such statutes and regulations applicable to the provision of Services, and the State and Eligible Public Entities are solely responsible for compliance with laws that apply to the State and Eligible Public Entities that would not ordinarily apply to the Contractor.

b) If this Contract is in excess of $554,000, it is subject to the requirements of the World Trade Organization (WTO) Government Procurement Agreement (GPA).

c) The State and Eligible Public Entities have an obligation to ensure that information technology is accessible to individuals with disabilities in accordance with the accessibility standards adopted under section 508 of the federal Rehabilitation Act of 1973, as amended, and its implementing regulations ("Section 508"). To the extent that this Contract falls within the scope of Government Code Section 11135, the Contractor hereby agrees to respond to and resolve any complaint brought to its attention, regarding accessibility of its Services. Upon request, Contractor may provide Eligible Public Entities with a completed Voluntary Product Accessibility Template (VPAT) of the specific product (or a URL to the VPAT) for reviewing compliance with Section 508 requirements. If Contractor is unable to provide a VPAT for a product or service, the parties acknowledge that the products or services may not be eligible for purchase by the Eligible Public Entity.

8. CONTRACTOR'S POWER AND AUTHORITY:

The Contractor warrants that it has full power and authority to grant the rights herein granted. Further, the Contractor avers that it will not enter into any arrangement with any third party which might abridge any rights of the State under this Contract.

9. ASSIGNMENT:

This Contract shall not be assignable by the Contractor in whole or in part without the written consent of the State. The State's consent shall not be unreasonably withheld or delayed. For the purpose of this paragraph, the State will not unreasonably prohibit the Contractor from freely assigning its right to payment, provided that the Contractor remains responsible for its obligations hereunder.

10. WAIVER OF RIGHTS:

Any action or inaction by the State or the failure of the State on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by the State

of its rights hereunder and shall not prevent the State from enforcing such provision or right on any future occasion. The rights and remedies of the State herein are cumulative and are in addition to any other rights or remedies that the State may have at law or in equity.

11. ORDER OF PRECEDENCE:

In the event of any inconsistency between the articles, attachments, specifications or provisions which constitute this Contract, the following order of precedence shall apply:

a) These FedRAMP Moderate Cloud Computing General Provisions-Information Technology, unless expressly superseded by language in the Contract;
b) Contract form, i.e., Purchase Order STD 65, Standard Agreement STD 213, etc., and any amendments thereto;
c) The FedRAMP Moderate Cloud Computing Special Provisions - Infrastructure as a Service and Platform as a Service {hereafter referred to as, the "Special Provisions");
d) Cost worksheets;
e) The CSP's service agreement and attachments; and
f) All other attachments incorporated in the Contract by reference.

12. WARRANTY:

a) Limited Warranty for Services. In addition to any warranties set forth in the agreement, Contractor warrants that:
   i. Services will be performed in accordance with the applicable service agreement and/or SLA; and
   ii. All customer support for Services will be performed with professional care and skill.
b) Such Limited Warranty will be for the duration of Customer's use of the Services, subject to the notice requirements set forth herein. This Limited Warranty is subject to the following limitations:
   i. any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law last for one year from the start of the limited warranty;
   ii. the limited warranty does not cover problems caused by accident, abuse or use in a manner inconsistent with this agreement or any applicable service agreement, or resulting from events beyond Contractor's reasonable control;
   iii. the limited warranty does not apply to components of Software products that the Eligible State Entity may be permitted to redistribute;
   iv. the limited warranty does not apply to free, trial, pre-release, or beta Services; and
   v. the limited warranty does not apply to problems caused by the failure to meet minimum system requirements.

c) **Remedies for breach of Limited Warranty.** If Contractor fails to meet any of the above limited warranties and Customer notifies Contractor within the warranty period, then the affected Eligible Public Entity shall be entitled to the following remedies:
   i. Service Credits and Performance Discounts as applicable;
   ii. Re-performance, repair or replacement. In the event the Contractor fails to re-perform, repair or replace the products and/or services as appropriate, the State may terminate the contract for default pursuant to Section 17; and

iii. Termination for default. These are Customer's only remedies for breach of the limited warranty, unless other remedies are required to be provided under applicable law or as maybe specifically provided elsewhere in this Contract.

d) **DISCLAIMER OF OTHER WARRANTIES.** OTHER THAN THIS LIMITED WARRANTY, CONTRACTOR PROVIDES NO OTHER EXPRESSOR IMPLIED WARRANTIES OR CONDITIONS. CONTRACTOR DISCLAIMS ANY IMPLIED REPRESENTATIONS, WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OF MERCHANTABLIITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR TITLE. THESE DISCLAIMERS WILL APPLY UNLESS APPLICABLE LAW DOES NOT PERMIT THEM.

e) Contractor shall apply anti-malware controls to the Services to help avoid malicious software gaining unauthorized access to State Data, including malicious software originating from public networks. Such controls shall at all times equal or exceed the controls consistent with the industry standards for such data, but in no event less than the controls that Contractor applies to its own internal corporate electronic data of like character.

f) Unless otherwise specified elsewhere in the Contract:
   i. The Contractor does not warrant that any Software provided hereunder is error-free or that it will run without immaterial interruption; and
   ii. The Contractor does not warrant and will have no responsibility for a claim to the extent that itarises directly from (A) a modification made by the State, unless such modification is approved or directed by the Contractor, (B) use of Software in combination with or on products other than as specified by the Contractor, or (C) misuse by the State.

g) All warranties, including special warranties specified elsewhere herein, shall inure to the State, its successors, assigns, customer agencies, and governmental users of the Deliverables or services.

14. SAFETY AND ACCIDENT PREVENTION:

In performing work under this Contract on State premises, the Contractor shall conform to any specific safety requirements contained in the Contract or as required by law or regulation. The Contractor shall take any additional precautions as the State may reasonably require for safety andaccident prevention purposes. Any violation of such rules and requirements, unless promptly corrected, shall be grounds for termination of this Contract in accordance with the default provisions hereof.

15. TERMINATION FOR NON-APPROPRIATION OF FUNDS:

a) If the term of this Contract extends into fiscal years subsequent to that in which it is approved, such continuation of the Contract is contingent on the appropriation of funds for such purpose by the Legislature. If funds to effect such continued payment are not appropriated, the Contractor agrees to terminate any services supplied to the State under this Contract, and relieve the State of any further obligation therefor.

b) The State agrees that if it appears likely that subsection a) above will be invoked, the State and Contractor shall agree to take all reasonable steps to prioritize work and Deliverables and minimize the incurrence of costs prior to the expiration of funding for this Contract.

16. TERMINATION FOR THE CONVENIENCE OF THE STATE:

a) The State may terminate performance of work under this Contract for its convenience in whole or, from time to time, in part, if the Department of General Services, Deputy Director Procurement Division, or designee, determines that a termination is in the State's interest. The Department of General Services, Deputy Director, Procurement Division, or designee, shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date thereof;

b) After receipt of a Notice of Termination, and except as directed by the State, the Contractor shall immediately stop work as specified in the Notice of Termination, regardless of any delay in determining or adjusting any amounts due under this clause;

c) After termination, the Contractor shall submit a final termination settlement proposal to the State in the form and with the information prescribed by the State except that in no instance shall the Contractor seek nor will the State pay for costs not specified on an order for services regardless of Contractors' liability or costs for materials, equipment, software, facilities, or sub-contracts. The Contractor shall submit the proposal promptly, but no later than 90 days after the effective date of termination, unless a different time is provided in the Statement of Work or in the Notice of Termination;

d) The Contractor and the State may agree upon the whole or any part of the amount to be paid as requested under subsection (c) above;

e) Unless otherwise set forth in the Statement of Work, if the Contractor and the State fail to agree on the amount to be paid because of the termination for convenience, the State will pay the Contractor the following amounts; provided that in no event will total payments exceed the amount payable to the Contractor if the Contract had been fully performed:

i. The Contract price for Deliverables or services accepted or retained by the State and not previously paid for; and

f) The Contractor will use generally accepted accounting principles, or accounting principles otherwise agreed to in writing by the parties, and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

17. TERMINATION FOR DEFAULT:

a) The State may, subject to the clause titled "Force Majeure", by written notice of default to the Contractor, terminate this Contract in whole or in part if the Contractor fails to:

i. Perform the Services within the time specified in the Contract or any amendment thereto;

ii. Make progress, so that the lack of progress endangers performance of this Contract; or

iii. Perform any of the other provisions of this Contract.

b) The State's right to terminate this Contract under subsection a) above, may be

exercised only if the failure constitutes a material breach of this Contract and if the Contractor does not cure such failure within the time frame stated in the State's cure notice, which in no event will be less than thirty (30) days, unless otherwise provided;

c) Both parties, State and Contractor, upon any termination for default, have a duty to mitigate the damages suffered by it. The State shall pay Contract price for completed and accepted Deliverables; and

d) The rights and remedies of the State in this clause are in addition to any other rights and remedies provided by law or under this Contract, and are subject to the clause titled "Limitation of Liability."

18. FORCE MAJEURE:

Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises from causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include, but are not limited to:

a) Acts of God or of the public enemy, and

b) Acts of the federal or State government in either its sovereign or contractual capacity.

If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform.

19. [RESERVED]

20. LIMITATION OF LIABILITY:

a) Except for the State's liability under Section 9 of the Service Agreement, each party's aggregate liability under this Contract for damages, shall be limited to the lesser of (i) the amounts paid in aggregate by the State and all Eligible Public Entities for all Services purchased over the 12 months before the liability arose; or (ii) $20 million (USD). Contractor's aggregate liability to the State under Section 29 (Patent, Copyright and Trade Secret Indemnity) arising out of the Services' alleged infringement or violation of intellectual property rights will not exceed $3 million. Nothing herein shall be construed to waive or limit the State's sovereign immunity or any other immunity from suit provided by law; and

b) IN NO EVENT WILL EITHER THE CONTRACTOR OR THE STATE BE LIABLE FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES, EVEN IF NOTIFICATION HAS BEEN GIVEN AS TO THE POSSIBILITY OF SUCH DAMAGES.

21. [RESERVED]

22. INVOICES:

Unless otherwise specified, invoices shall be sent to the address set forth herein. Invoices shall be submitted in triplicate and shall include the Contract number; release order number (if applicable); item number; unit price, extended item price and invoice total amount. State sales tax and/or use tax shall be itemized separately and added to each invoice as applicable.

23. REQUIRED PAYMENT DATE:

Payment will be made in accordance with the provisions of the California Prompt Payment Act, Government Code Section 927 et. seq. Unless expressly exempted by statute, the Act requires Stateagencies to pay properly submitted, undisputed invoices not more than 45 days after:

a) the date of acceptance of Deliverables or performance of services; or
b) receipt of an undisputed invoice, whichever is later.

24. TAXES:

Unless otherwise required by law, the State of California is exempt from Federal excise taxes. The State will only pay for any State or local sales or use taxes on the services rendered or Goods supplied to the State pursuant to this Contract.

25. CONTRACT MODIFICATION:

Contractor shall provide thirty (30) days written notice prior to modification of any service agreement terms. No amendment or variation of the terms of this Contract shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or agreement not incorporated in the Contract is binding on any of the parties.

26. CONFIDENTIALITY OF DATA:

All State Data, as defined herein, made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The Contractor shall not be required under the provisions of this paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession without obligation

of confidentiality, is independently developed by the Contractor outside the scope of this Contract, or is rightfully obtained from third parties.'

27. NEWS RELEASES

Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this Contract shall not be made without prior written approval of the Department of General Services.

28. PROTECTION OF PROPRIETARY SOFTWARE AND OTHER PROPRIETARY DATA:

a) The State agrees that all material appropriately marked or identified in writing as proprietary and furnished hereunder by the Contractor are provided for the State's exclusive use for the purposes of this Contract only. All such proprietary data shall remain the property of the Contractor. The State agrees to take all reasonable steps to ensure that such proprietary data are not disclosed to others, without prior written consent of the Contractor, subject to the California Public Records Act;

b) The State will insure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed; and

c) The State agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to proprietary data to satisfy its obligations in this Contract with respect to use, copying, modification, protection and security of proprietary materials and data, subject to the California Public Records Act.

29. PATENT, COPYRIGHT AND TRADE SECRET INDEMNITY:

a) Subject to the limitation of liability and warranty disclaimers under this Contract, Contractor will reimburse the State, its officers, agents and employees, for their respective out-of-pocket costs (including without limitation reasonable attorney's fees) incurred to defend any lawsuit brought against the State by an unaffiliated third party for infringement or violation of any U.S. Intellectual Property Right by Services provided hereunder ("IP Claim"), and will indemnify the State, its officers, agents and employees for the amount of any adverse final judgment or settlement arising out of an IP Claim.
The payment obligations set forth in the Section will be conditioned upon the following:
   i. The State will notify the Contractor of any such claim in writing and tender the defensethereof within a reasonable time; and
   ii. The State may not consent to the entry of any judgment or enter into any settlement with respect to the claim without prior written notice to the Contractor. The Contractor may assume control of or otherwise participate in the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (a) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (b) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (c)

the State will reasonably cooperate in the defense and in any related settlement negotiations.

b) Should the Services, or the operation thereof, become, or in the Contractor's opinion are likely to become, the subject of a claim of infringement or violation of a U.S. Intellectual Property Right, the State shall permit the Contractor, at its option and expense, either
   i. procure the right to continue using the Services alleged to be infringing;
   ii. replace or modify the same so that they become non-infringing ;or
   iii. immediate terminate the alleged infringing portion of the Services.

   If none of these options can reasonably be taken, or if the use of such Services by the State shallbe prevented by injunction, the Contractor agrees to make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the use of other Services acquired from the Contractor under this Contract is impractical, the State shall have the option of terminating such Contractor or orders, or applicable portions thereof, without penalty or termination charge. The Contractor agrees to refund any sums the State has paid the Contractor for unused Services.

c) This section constitutes the State's sole and exclusive remedy and Contractor's entire obligation to the State with respect to any claim that the Services infringe rights of any third party. The Contractor shall have obligations under this provision only for IP claims and final awards for the infringement of intellectual property right caused solely by the Services, and shall have no liability to the State under any provisions of this clause with respect to any claim of patent, copyright or trade secret infringement which is based upon:
   i. The unauthorized use or modification initiated by the State, User or a third party with or without State direction or approval, of any Service furnished hereunder;
   ii. The combination or utilization of Software furnished hereunder with non-Contractor supplied Software;
   iii. Any use of Services, or any other act by the State or Users, that is in breach of this Agreement;
   iv. Any claim of inducement or contributory negligence;
   v. Any claim of willful infringement directed any anyone other than the Contractor or the CSP;
   vi. Any use of the Services after the CSP has notified the State or Users to discontinue such use; or
   vii. The combination or utilization of Services furnished hereunder with any other equipment, service, data, Software or devices not made or furnished by the Contractor (including Third Party Content as defined the Service Agreement).

30. DISPUTES:

For disputes involving purchases made under this Agreement, to the extent permitted by applicable law, the Department of General Services, Procurement Division ("DGS") shall act on behalf of the State party or entity involved with the dispute. DGS in cooperation with the State party or entity involved with the dispute shall seek to resolve the dispute with Contractor on behalf of the State party or entity. The Contractor and DGS shall deal in good faith and attempt to resolve potential disputes informally through face-to-face negotiations with persons fully authorized to resolve the dispute or through non-binding mediation utilizing a mediator agreed to by the parties, rather than through litigation. No

formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief may begin until either such persons conclude, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely.

Notwithstanding the existence of a dispute under, related to or involving this Contract, the parties shall continue without delay to carry out all of their responsibilities, including providing of Services in accordance with the State's instructions regarding this Contract. Contractor's failure to diligently proceed in accordance with the State's instructions regarding this Contract that are not affected by the dispute shall be considered a material breach of this Contract.

31. EXAMINATION AND AUDIT:

The Contractor agrees that the State or its designated representative shall have the right to review and copy any records and supporting documentation directly pertaining to performance of this Contract. The Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. The Contractor agrees to allow the auditor(s) access to such records during normal business hours and in such a manner so as to not interfere unreasonably with normal business activities and to allow interviews of any employees or others who might reasonably have information related to such records to the extent necessary to verify the accuracy of such statements. Any such audit must: (i) not be disruptive to Contractor business and must take place at a mutually agreed time during Contractor's normal business hours; and (ii) take place on at least thirty (30) days' prior written notice. The State agrees that any information learned or disclosed by the State's auditor in connection with any such audit is Confidential Information of the Contractor and subject to nondisclosure and nonuse obligations under the NDA except as such disclosure or use is required by the California Public Records Act or other applicable law. The State will be solely responsible for all costs of any audit he State conducts. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract for performance of this Contract. Audits of data centers shall be in accordance with the Data Center Audit provisions in the Special Provisions. For clarity, from time to time, the Contractor may retain external auditors to verify its security measures (e.g., in a Service Organization Controls 1, Type 2 report or its equivalent, as determined by Contractor). Upon State's request, Contractor will provide to State a copy of the report(s) ("Reports") issued by the external auditors. The Reports might include various reports or certifications, such as (by way of example) a Service Organization Controls 1, Type 2 report, or an ISO 27001 certificate, or such other industry standard reports or certifications that cover comparable standards or controls as defined by Contractor. Contractor will provide such Reports no more frequently than twice annually. Reports are subject to availability and will be treated as Confidential Information of Contractor under the NDA. Audits of data centers shall be in accordance with the Data Center Audit provisions in the Special Provisions.

32. PRIORITY HIRING CONSIDERATIONS:

If this Contract includes services in excess of $200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with PCC Section 10353. The State acknowledges that no positions are funded by the Contract within the meaning of this provision.

33. COVENANT AGAINST GRATUITIES:

The Contractor warrants that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by the Contractor, or any agent or representative of the Contractor, to any officer or employee of the State with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the State shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the State in procuring on the open market any items which the Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of the State provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or in equity.

34. NONDISCRIMINATION CLAUSE:

a) During the performance of this Contract, the Contractor and its subcontractors shall not unlawfully discriminate, harass or allow harassment, against any employee or applicant for employment because of sex, sexual orientation, race, color, ancestry, religious creed, national origin, disability (including HIV and AIDS), medical condition (cancer), age, marital status, and denial of family care leave. The Contractor and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. The Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12990 et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations are incorporated into this Contract by reference and made a part hereof as if set forth in full. The Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.

b) The Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform Services under the Contract.

35. NATIONAL LABOR RELATIONS BOARD CERTIFICATION:

The Contractor swears under penalty of perjury that no more than one final, unappealable finding of contempt of court by a federal court has been issued against the Contractor within the immediately preceding two-year period because of the Contractor's failure to comply with an order of the National Labor Relations Board. This provision is required by, and shall be construed in accordance with, PCC Section 10296.

36. ASSIGNMENT OF ANTITRUST ACTIONS:

Pursuant to Government Code Sections 4552, 4553, and 4554, the following provisions are incorporated herein:

a) In submitting a bid to the State, the supplier offers and agrees that if the bid is accepted, it will assign to the State all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. 15) or under the Cartwright Act (Chapter 2, commencing with Section 16700, of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of Goods, material or other items, or services by the supplier for sale to the State pursuant to the solicitation. Such assignment shall be made and become effective at the time the State tenders final payment to the supplier. The State acknowledges that the Contract is only for Contractor's Services and that Contractor does not purchase goods, material, other items, or services and then resell the same to the State under this Contract.

b) If the State receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the State any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the State as part of the bid price, less the expenses incurred in obtaining that portion of the recovery.

c) Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and

(i) the assignee has not been injured thereby, or

(ii) the assignee declines to file a court action for the cause of action.

37. DRUG-FREE WORKPLACE CERTIFICATION:

The Contractor certifies under penalty of perjury under the laws of the State of California that the Contractor will comply with the requirements of the Drug- Free Workplace Act of

1990 (Government Code Section 8350 et seq.) and will provide a drug-free workplace by taking the following actions:

a) Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).

b) Establish a Drug-Free Awareness Program as required by Government Code Section 8355(b) to inform employees about all of the following:

(i) the dangers of drug abuse in the workplace;

(ii) the person's or organization's policy of maintaining a drug-free workplace;

(iii) any available counseling, rehabilitation and employee assistance programs; and,

(iv) penalties that may be imposed upon employees for drug abuse violations.

c) Provide, as required by Government Code Section 8355(c), that every employee who works on the proposed or resulting Contract:

(i) will receive a copy of the company's drug-free policy statement; and,

(ii) will agree to abide by the terms of the company's statement as a condition of employment on the Contract.

38. FOUR-DIGIT DATE COMPLIANCE:

Contractor warrants that the Services can be used by the State to provide only Four-Digit Date Compliant (as defined below) Services. "Four Digit Date Compliant" Services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.

39. COMPLIANCE WITH PUBLIC CONTRACT CODE SECTION 6108:

Contractor agrees that it complies with Public Contract Code Section 6108, to the extent applicable.

40. [RESERVED]

41. CHILD SUPPORT COMPLIANCE ACT:

For any Contract in excess of $100,000, the Contractor acknowledges in accordance with PCC Section 7110, that:

a) The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable State and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with Section 5200) of Part 5 of Division 9 of the Family Code; and

b) The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.

42. AMERICANS WITH DISABILITIES ACT:

The Contractor assures the State that the Contractor complies with the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.).

43. [RESERVED]

44. [RESERVED]

45. EXPATRIATE CORPORATIONS:

Contractor hereby declares that it is not an expatriate corporation or subsidiary of a non-US expatriate corporation within the meaning of PCC Sections 10286 and 10286.1, and is eligible to contract with the State.

46. DOMESTIC PARTNERS:

For contracts over $100,000 executed or amended after January 1, 2007, the contractor certifies that the Contractor is in compliance with Public Contract Code Section 10295.3.

47. SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:

a) If for this Contract the Contractor made a commitment to achieve small business participation, then the Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) report to the awarding department the actual percentage of small business participation that was achieved. (Govt. Code § 14841.)

b) If for this Contract the Contractor made a commitment to achieve disabled veteran business enterprise (DVBE) participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be

specified elsewhere in this Contract) certify in a report to the awarding department: (1) the total amount the prime Contractor received under the Contract; (2) the name and address of the DVBE(s) that participated in the performance of the Contract; (3) the amount each DVBE received from the prime Contractor; (4) that all payments under the Contract have been made to the DVBE; and (5) the actual percentage of DVBE participation that was achieved. A person or entity that knowingly provides false information shall be subject to a civil penalty for each violation. (Mil. & Vets. Code § 999.5(d); Govt. Code § 14841.)

48. LOSS LEADER:

It is unlawful for any person engaged in business within this state to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code. (PCC 12104.5(b).).

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT F

FEDRAMP MODERATE CLOUD COMPUTING SPECIAL PROVISIONS

(INFRASTRUCTURE AS A SERVICE AND PLATFORM AS A SERVICE)

These FedRAMP Moderate Cloud Computing Special Provisions (Infrastructure as a Service and Platform as a Service) ("FedRAMP Mod Cloud Special Provisions") shall apply to all EligiblePublic Entities' use of permitted Services and /or products.

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IAAS) AND PLATFORM AS A SERVICE (PAAS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE FEDRAMP MODERATE CLOUD COMPUTING GENERAL PROVISIONS - INFORMATION TECHNOLOGY (THE "GENERAL PROVISIONS") AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA).
STATE AGENCIES MUST FIRST:

a) CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;
b) CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;
c) MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. DEFINITIONS:

a) **"Authorized Persons"** means the Service Provider's employees, contractors, subcontractors or other agents who need to access the State's Data to enable the service provider to perform the services required.
b) **"Data Breach"** means any unlawful access, use, theft or destruction to any State Data stored on the CSP's equipment or facilities, or unauthorized access to such equipment or facilities that results in the use, disclosure, destruction, alteration, loss or theft of State Data.
c) **"Security Incident"** is synonymous with Data Breach.
d) **"Service Level Agreement" (SLA)** means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document thatunless otherwise agreed to includes: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, and (4) any remedies for performance failures.
e) **State Identified Contact"** means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification. For purposes of this Contract, State Identified Contacts shall be individuals that are registered by the State as administrators in the Service Provider's administrative portal. For clarity, if more than one administrator is identified by the State, the Service Provider may only contact one of them.

2. DATA OWNERSHIP:

The State will own all right, title and interest in all State Data. The Service Provider shall not access State user accounts or State Data, except:

a) in the course of data center operations;
b) in response to service or technical issues;
c) as required by the express terms of this Contract;
d) at the State's written request; or
e) as required by law.

3. DATA PROTECTION:

The Service Provider and the State recognize that security responsibilities are shared. The Service Provider is responsible for implementing security measures and providing a secure infrastructure (i.e., the AWS Network) as set forth in the Service Agreement and AWS Security Standards attached thereto. The State is responsible for all other data protection and security controls, including its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the Service Agreement, the SOW and/or SLA.

a) All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State.

b) The Service Agreement, SOW and/or SLA will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the Service Agreement, SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.

c) At no time shall any State Data or processes - which either belong to or are intended for the use of State or its officers, agents or employees - be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State except as expressly permitted by the Service Agreement or Section 2 above.

d) The State and Eligible Public Entities shall enter into and comply with a Business Associate Agreement in using the Services to store or transmit any Protected Health Information.

e) As of the Addendum Effective Date, the Service Provider is authorized under FedRAMP Moderate ("FedRAMP" for the purpose of this section) in accordance with Exhibit B and as provided in https://aws.amazon.com/compliance/services-in-scope/ or its successor webpage designated by the Service Provider (the "Services in Scope Site") for ATOs by Service, region, and impact level. AWS GovCloud (US), has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate and high impact levels. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at high baseline security categorization can be found within the Services in Scope Site.

The Service Provider achieves FedRAMP compliance by addressing the FedRAMP security controls (based on NIST SP 800-53), using required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, completing FedRAMP accredited independent third party (3PAO) security testing and evaluation and submitting continuous monitoring requirements of FedRAMP to the Joint Authorization Board (JAB). It is exclusively the State's and Eligible Public Entities' responsibility to leverage the relevant FedRAMP authorized Services and to select and maintain all State Data within the relevant authorized regions in order to leverage the foregoing authorizations.

4. DATA LOCATION:

The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be locatedsolely in data centers in the continental United States. The Service Provider shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical user support or other customer support. The Service Provider may provide technical user support or other customer support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract.

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

Subject to the requirement to register administrator contact information, as set forth in thefollowing paragraph, if the CSP becomes aware of a Security Incident (which, for the purposes of this Contract, shall be synonymous with Data Breach, as defined above), theCSP will immediately investigate the Security Incident, and as soon as possible and no later than seventy-two (72) hours after the service provider determines that a Security Incident has occurred: (1) notify one or more State Identified Contacts of the Security Incident; (2) provide the State with detailed information about the Security Incident; and (3) take commercially reasonable measures to mitigate the effects and to minimize any damage resulting from the Security Incident. The CSP and Contractor shall reasonably cooperate fully with the State, its agents and law enforcement in investigating any such security incident.

Notification(s) of Security Incidents will be delivered to one or more of the State's administrators (see definition of State Identified Contact, above) by any means the CSP selects, including via email. It is the State's sole responsibility to ensure its administrators maintain accurate contact information on the CSP's service portal.

The CSP's obligation to report or respond to a Security Incident under this section is not anacknowledgement by the service provider of any fault or liability with respect to the Security Incident.

The State must notify the CSP promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

SECURITY INCIDENT RESPONSIBILITIES:

If requested by the Eligible Public Entity by contacting the Service Provider Contracts Management team at: aws-californiastate@amazon.com (or other email address as may be specified by AWS), Service Provider will provide the Eligible Public Entity with reasonable and appropriate details relevant to the cause, nature and Eligible Public Entity impact of the Security Incident; provided that Service Provider will not be required to provide this information if the Service Provider reasonably determines the disclosure would prejudice Service Provider's security or violate applicable law. Service Provider will reasonably cooperate with Eligible Public Entities to support inquiries following a Security Incident as permitted under the circumstances.

6. NOTIFICATION OF LEGAL REQUESTS:

Service Provider shall not respond to legal requests directed at the State or Eligible PublicEntities on behalf of the State or the Eligible Public Entities, unless authorized in writing. Unless otherwise prohibited by law or relevant court or governmental order, the Service Provider shall contact the State or the relevant Eligible Public Entity within a reasonable time before disclosing State Data in response to any electronic discovery requests, litigation holds, discovery searches, expert testimonies or California Public Records Actrequests, directed at the Service Provider requesting that the Service Provider disclose State Data submitted under this Contract.

Except as the State directs, Service Provider will not provide any third party: (1) direct, indirect, blanket or unfettered access to State Data; (2) the platform encryption keys usedto secure State Data or the ability to break such encryption; or (3) any kind of access to State Data if Service Provider is aware that such data is used for purposes other than those stated in the request.

In support of the above, Service Provider may provide the State (and/or the relevant Eligible Public Entity's) basic contact information to the third party.

7. DATA PRESERVATION AND RETRIEVAL:

For ninety (90) days following the expiration date (or early termination date) of this Contract ("Retention Period"), or upon notice of termination of this Contract, Service Provider shall provide the State self-service access to State Data.

Upon request by the State at least 30 days prior to expiration, and in the event that the State does not choose to renew the Contract and subscription for a longer term as provided in the Contract, Service Provider will make arrangements for the State (or its contractor, if applicable) to extend its Contract and paid subscription for the IaaS and/or PaaS services, for a 90-day period, during which the services will retain their normal functionality.

Notwithstanding any provision to contrary in the Service Provider's SOW or the SLA, no additional fees shall be imposed on the State or Eligible Public Entity for access and dataretrieval during the 90-day period prior to termination.

During any Retention Period, and any period of service suspension, the Service Provider shall not take any action to intentionally erase any State Data, and access to State Datashall continue to be made available to the State or the Eligible Public Entities without alteration.

The State or Eligible Public Entities shall be responsible for retrieving and/or destroying State Data stored using the Services when no longer required by law, by taking steps within their control to destroy any State Data that includes personal information or to ensure that such information is de-identified.

8. BACKGROUND CHECKS:

The Service Provider shall conduct criminal background checks on its Authorized Persons andnot provide access to State Data to any persons who fail such background checks, in accordance with the requirements of FedRAMP (Moderate Specification) and any US

Federal Government regulation that Service Provider's IaaS and/or PaaS services are subject to. The Service Provider shall promote and maintain an awareness of the importance of securing State Data among the Service Provider's employees and agents.

9. ACCESS TO SECURITY LOGS AND REPORTS:

Service Provider shall allow the State and Eligible Public Entities reasonable self-service access to security logs, information, latency statistics, data, and other related security data that affect this Contract and State Data, at no cost to the State and Eligible Public Entities. The parties recognize that the type of self-service access and security data made availableto the State may be subject to change.

10. CONTRACT AUDIT:

The Service Provider shall allow the State to audit conformance to the Contract terms. The State may perform this audit or Contract with a third party at its discretion and at the State's expense. Any such third party hired by the State shall enter into a Non-Disclosure Agreement with terms no less restrictive than the NDA between the State and Contractor.

11. DATA CENTER AUDIT:

From time to time, but at least once a year, the Service Provider shall retain external auditors to verify its security measures at its own expense. The Service Provider shall provide a version of the report issued by the external auditors, may not be redacted, upon request. In the event the audit report contains the Service Provider's proprietary information, the State acknowledges that such information is Confidential Information and the audit report shall be disclosed only upon execution of a mutual non-disclosure agreement. If the State of Eligible Public Entity receives a California Public Records Act request for the audit report, the State and Eligible Public Entity shall provide the Service Provider reasonable written notice to permit the Service Provider to enable the Service Provider to steps to prevent the disclosure of such information to the maximum extent permitted by law. State shall be limited to no more than two audits annually.

12. CHANGE CONTROL AND ADVANCE NOTICE:

The Service Provider shall give sixty (60) days advance written notice to the State of any discontinuance of a Service or functionality of a Service that is generally makes available to its customers. Service Provider may change the features and functionality of the Services to make improvements, address security requirements and comply with changes in law, without prior notice.

13. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes to the State such that adequate protection and flexibility can be attained between the State and the Service Provider.

14. IMPORT AND EXPORT OF DATA:

During the term of a subscription or any Retention Period, the State shall have the ability toimport or export data in whole or in part at its discretion without interference from the Service Provider.

15. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the Service Provider. Unless otherwise provided, the system shall be available 24/7/365 (except for scheduled maintenance downtime), and shall provide service to customers as described in the Contract.

16. RIGHT TO REMOVE INDIVIDUALS:

The State shall have the right at any time to require the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State shall provide theService Provider with notice of its determination, and the reasons it requests the removal. The Service Provider shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

17. BUSINESS CONTINUITY AND DISASTER RECOVERY:

The Service Provider shall maintain and regularly test a business continuity and disasterrecovery program as it pertains to the Services.

18. WEB SERVICES:

The Service Provider shall use web service exclusively to interface with State Data in nearreal time when possible, or as mutually agreed.

EXHIBIT G
AWS SERVICE AGREEMENT

This AWS Service Agreement (this "**Agreement**") is made and entered into and a part of contract no. 20-14328 ("**Contract**"). In addition to other parts of the Contract, this Service Agreement applies to all Eligible Public Entities ("**Customer**").

In consideration of the mutual promises contained in this Agreement, AWS and Customer agree to all terms of the Agreement effective as of the date of the Contract.

Defined terms used in this Agreement with initial letters capitalized have the meanings given in Section 13 below.

1. Use of the Service Offerings.

1.1 Generally. Customer may access and use the Service Offerings in accordance with this Agreement and contract No. 20-14328 between AWS and the State of California, acting by and through the California Department of General Services (the "**Contract**"). Service Level Agreements may apply to certain Service Offerings. Customer will comply with the terms of this Agreement and all laws, rules, and regulations applicable to Customer's use of the Service Offerings.

1.2 AWS Account. To access the Services, Customer must create one or more AWS Enterprise Accounts. Unless explicitly permitted by the Service Terms, Customer will only create one AWS Enterprise Account per email address. Customer shall identify to AWS all Enterprise Accounts to be covered by this Agreement and the Contract. For all AWS Enterprise Accounts, this Agreement supersedes any acceptance of the AWS Customer Agreement by Customer or any of its employees acting on behalf of Customer. If Customer opens any AWS accounts that do not meet the definition of an "AWS Enterprise Account," those accounts will be governed by the AWS Customer Agreement.

1.3 Third-Party Content. Third-Party Content may be used by Customer at Customer's election. Third-Party Content is governed by this Agreement unless accompanied by separate terms and conditions, which may include separate fees and charges.

1.4 Eligible Public Entity. Any Eligible Public Entity (as defined in the Contract) may use the Service Offerings under its own AWS Enterprise Account(s) under the terms of this Agreement and the Contract. "Public Entity", as used in this part, means the sate, county, city, city and county, district, public authority, public agency, municipal corporation, or any other political subdivision or public corporation in the state.

2. Changes.

2.1 To the Service Offerings. AWS may change or discontinue any of the Service Offerings or change or remove functionality of any or all of the Service Offerings from time to time. AWS will provide at least 12 months prior Notice to Customer for any AWS Enterprise Accounts enrolled in AWS Support at the Developer-level tier or above (or any successor service providing such communications alerts) if AWS decides to discontinue a Service or functionality of a Service that it makes generally available to its customers, except that AWS will not be obligated to provide such Notice if the discontinuation is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity. Where AWS is excused from providing such Notice for the reasons given in this Section, AWS will make

commercially reasonable efforts to provide Notice to Customer as is reasonably practicable under the circumstances.

2.2 To APIs. AWS may change or discontinue any APIs for the Services from time to time. For any change or discontinuation of an API that is not also a discontinuation of a Service or a functionality of a Service, AWS will continue supporting the previous version of such API for 12 months after the change or discontinuation (except if doing so (a) would pose a security or intellectual property issue, (b) is technically infeasible, or (c) would prevent AWS from complying with the law or requests of governmental entities).

2.3 To the Service Level Agreements. AWS may change or add Service Level Agreements from time to time, but will provide 90 days advance Notice to Customer before materially reducing the benefits offered to Customer under any of the Service Level Agreement(s) that are available as of the Effective Date.

3. Privacy and Security.

3.1 AWS Security. AWS will implement reasonable and appropriate measures for the AWS Network (as determined by AWS) designed to help Customer secure Customer Content against accidental or unlawful loss, access or disclosure (the "**Security Objectives**") in accordance with the AWS Security Standards. AWS may modify the AWS Security Standards from time to time, but will continue to provide at least the same level of security as is described in the AWS Security Standards on the Effective Date.

3.2 Data Privacy. Customer may specify the AWS regions in which Customer Content will be stored. Customer consents to the storage of Customer Content in, and transfer of Customer Content into, the AWS regions Customer selects. AWS will not access or use Customer Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. AWS will not (a) disclose Customer Content to any government or third party, or (b) subject to Section 3.3, move Customer Content from the AWS regions selected by Customer; except in each case as necessary to comply with the law or a binding order of a governmental body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, AWS will give Customer reasonable Notice of any legal requirement or order referred to in this Section 3.2, to allow Customer to seek a protective order or other appropriate remedy. AWS will only use Account Information in accordance with the Privacy Policy, and Customer consents to such usage. The Privacy Policy does not apply to Customer Content.

3.3 Service Attributes. To provide billing and administration services, AWS may process Service Attributes in the AWS region(s) where Customer uses the Service Offerings and the AWS regions in the United States. To provide Customer with support services initiated by Customer and investigate fraud, abuse or violations of this Agreement, AWS may process Service Attributes where AWS maintains its support and investigation personnel.

4. Customer Responsibilities.

4.1 Customer Accounts. Except to the extent caused by AWS's breach of this Agreement, (a) Customer is responsible for all activities that occur under its AWS Enterprise Accounts, regardless of whether the activities are authorized by Customer or are undertaken by Customer, its employees or a third party (including without limitation contractors, agents or End Users), and (b) AWS and its Affiliates are not responsible for unauthorized access to Customer's AWS Enterprise Accounts.

4.2 Customer Content. Customer will ensure that Customer Content, Customer Submissions or Customer/End Users' use of Customer Content, Customer Submissions or the Service

Offerings will not violate any of the Policies or any applicable law. Customer is solely responsible for the development, content, operation, maintenance, and use of Customer Content and Customer Submissions. For example, Customer is solely responsible for:

(a) the technical operation of Customer Content, including ensuring that calls Customer makes to any Service are compatible with then-current APIs for that Service, including any APIs AWS continues to support under Section 2.2 of this Agreement;

(b) any claims relating to Customer Content or Customer Submissions; and

(c) properly handling and processing notices that are sent to Customer (or any Customer Affiliate) regarding Customer Content or Customer Submissions, such as by any person claiming that Customer Content or Customer Submissions violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act.

4.3 Customer's Security and Redundancy. Customers have a variety of options to choose from when configuring their accounts, and for all sensitive or otherwise valuable content AWS recommends that Customer uses strong security and redundancy features, such as access controls, encryption, and backup. Customer is responsible for properly configuring and using the Service Offerings in a manner that provides security and redundancy of its AWS Enterprise Accounts and Customer Content, such as, for example, using enhanced access controls to prevent unauthorized access to AWS Enterprise Accounts and Customer Content, using encryption technology to prevent unauthorized access to Customer Content, and ensuring the appropriate level of backup to prevent loss of Customer Content.

4.4 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for Customer's internal use only and Customer may not sell, transfer or sublicense them to any other entity or person, except that Customer may disclose its private key to its agents and subcontractors (including any of its Affiliates who are acting as an agent or subcontractor of Customer) performing work on behalf of Customer.

4.5 End Users. Customer is responsible for End Users' use of Customer Content and the Service Offerings. Customer will ensure that all End Users comply with Customer's obligations under this Agreement and that the terms of its agreement with each End User are not inconsistent with this Agreement. If Customer becomes aware of any violation of its obligations under this Agreement by an End User, Customer will immediately suspend access to Customer Content and the Service Offerings by such End User, person or entity. AWS does not provide any support or services to End Users unless AWS has a separate agreement with Customer or an End User obligating AWS to provide support or services. Customer is responsible for providing customer service (if any) to End Users. The Customer receives Basic Support included with its AWS account and may engage in additional tiers of support, as provided on the AWS Support website (or its successor site): (currently located at https://aws.amazon.com/premiumsupport/).

5. Fees and Payment.

5.1 Service Fees. Unless otherwise stated on the AWS Site, AWS will invoice Customer at the end of each month for all applicable fees and charges accrued for use of the Service Offerings, as described on the AWS Site, during the month. Customer will pay AWS all invoiced amounts within 45 days of the date of the invoice (other than Disputed Amounts). Payment will be made in accordance with the provisions of the California Prompt Payment Act, including any provisions granting a contractor interest for late payments. For any Disputed Amounts, Customer will provide Notice to AWS, including the basis for the dispute (including any supporting documentation), and the parties will meet within 30 days of the date of the Notice to resolve the dispute. If the parties fail to resolve the dispute within such 30 day period, AWS may, at its option, (a) suspend Customer's or any End User's right to access or use any portion or all of the Service Offerings,

immediately upon notice to Customer, and (b) terminate this Agreement pursuant to Section 7.2(b). All amounts payable by Customer under this Agreement will be paid to AWS without setoff or counterclaim and without deduction or withholding, provided that Disputed Amounts will be handled as set forth above. Fees and charges for any new Service or new feature of a Service will be effective when AWS posts updated fees and charges on the AWS Site, unless expressly stated otherwise in a Notice. AWS may increase or add new fees and charges for any existing Service by giving Customer at least 60 days advance Notice. .

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under this Agreement. All fees payable by Customer are exclusive of Indirect Taxes. AWS may charge and Customer will pay applicable Indirect Taxes that AWS is legally obligated or allowed to collect from Customer. Customer will provide such information to AWS as reasonably required to determine whether AWS is obligated to collect Indirect Taxes from Customer. AWS will not collect, and Customer will not pay, any Indirect Tax for which Customer furnishes AWS a properly completed exemption certificate or a direct payment permit certificate for which AWS may claim an available exemption from such Indirect Tax. All payments made by Customer to AWS under this Agreement will be made free and clear of any withholding or deduction for taxes. If any such taxes (for example, international withholding taxes) are required to be withheld on any payment, Customer will pay such additional amounts as are necessary so that the net amount received by AWS is equal to the amount then due and payable under this Agreement. AWS will provide Customer with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Agreement.

6. Temporary Suspension

6.1 Generally. AWS may suspend Customer's or any End User's right to access or use any portion of or all of the Service Offerings immediately upon Notice to Customer if AWS reasonably determines:

(a) Customer's or an End User's use of the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) risks adversely impacting AWS's systems, the Service Offerings or the systems or Content of any other AWS customer, or (iii) risks subjecting AWS or its Affiliates to liability; or

(b) Customer or any End User is not in compliance with the Acceptable Use Policy or Section 8 of this Agreement.

AWS will use commercially reasonable efforts to restore Customer's rights to use and access those portions of the Service Offerings or accounts that gave rise to the suspension promptly after Customer has resolved the problem giving rise to the suspension.

6.2 Effect of Suspension. If AWS suspends Customer's right to access or use any portion of the Service Offerings:

(a) Customer remains responsible for all fees and charges Customer incurs during the period of suspension; and

(b) Customer will not be entitled to any service credits under the Service Level Agreements for any period of suspension.

7. Term; Termination

7.1 Term. The term of this Agreement will commence on the Effective Date of the Contract and will remain in effect until terminated pursuant to this Agreement. Any Notice of termination of this Agreement by either party to the other must include a Termination Date.

7.2 Termination of Individual Enterprise Accounts.

(a) **Termination for Convenience.** Customer may terminate individual Enterprise Accounts for any reason by providing AWS Notice.

(b) **Termination for Cause.**

(i) **By Either Party.** Either party may terminate individual Enterprise Accounts for cause if the other party is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of Notice by the other party.

(ii) **By AWS.** AWS may also terminate individual Enterprise Accounts for cause upon 30 days Notice to Customer: (A) if there is an act or omission by Customer or any End User that AWS has the right to suspend for under Section 6 and, for those suspendable acts or omissions that are curable, Customer has not cured such condition within such 30 day period; or (B) in order to comply with applicable law or requests of governmental entities.

7.3 Effect of Termination.

(a) **Generally.** Upon the Termination Date:

(i) except as provided in Section 7.3(b), all of Customer's rights under this Agreement immediately terminate;

(ii) Customer remains responsible for all fees and charges Customer has incurred through the Termination Date;

(iii) Customer will immediately return or, if instructed by AWS, destroy all AWS Content in Customer's possession (except for AWS Content that is publicly available on the AWS Site); and

(iv) Sections 4, 5, 7.3, 8.1, 8.2, 8.4, 8.5, 9, 10, 11, 12 and 13 will continue to apply in accordance with their terms.

(b) **Post-Termination Retrieval of Customer Content.** During the 90 days following the Termination Date, AWS will not take action to remove any Customer Content as a result of the termination. In addition, during the 90 days following the Termination Date, AWS will allow Customer to retrieve any remaining Customer Content from the Services, unless (i) prohibited by law or the order of a governmental or regulatory body or it could subject AWS or its Affiliates to liability, or (ii) Customer has not paid all amounts due under this Agreement, other than Disputed Amounts. For any use of the Services during the 90 days following the Termination Date, the terms of this Agreement will apply and Customer will pay the applicable fees at the rates under Section 5. No later than the end of this 90-day period, Customer will close all AWS Enterprise Accounts, unless the parties agree on additional time.

8. Proprietary Rights.

8.1 Customer Content. As between Customer and AWS, Customer (or Customer's licensors) own all right, title, and interest in and to Customer Content. Except as provided in this Agreement, AWS obtains no rights under this Agreement from Customer (or Customer's licensors) to Customer Content.

8.2 Customer Submissions. Customer Submissions will be governed by the terms of the Apache License, Version 2.0, unless Customer requests and AWS consents in writing to another license supported by AWS.

8.3 Service Offerings License. As between Customer and AWS, AWS, its Affiliates or its licensors own all right, title, and interest in and to the Service Offerings, and all related technology and intellectual property rights. Subject to the terms of this Agreement, AWS grants Customer a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to do the following during the Term: (a) access and use the Services solely in accordance with this Agreement; and (b) copy and use the AWS Content solely in connection with Customer's permitted use of the Services. Except as provided in this Section 8.3, Customer obtains no rights under this Agreement from AWS, its Affiliates, or their licensors to the Service Offerings, including without limitation any related intellectual property rights. Some AWS Content may be provided to Customer under a separate license, such as the Apache License, Version 2.0, which will be identified to Customer in the notice file or on the download page, in which case that license will govern Customer's use of that AWS Content.

8.4 License Restrictions. Neither Customer nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither Customer nor any End User may, or may attempt to (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content included in the Service Offerings (except to the extent Content included in the Service Offerings are provided to Customer under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the Service Offerings or apply any other process or procedure to derive the source code of any software included in the Service Offerings, (c) access or use the Service Offerings in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (d) resell or sublicense the Service Offerings. During and after the Term, Customer will not assert, nor will Customer authorize, assist, or encourage any third party to assert, any intellectual property infringement claim regarding any Service Offerings Customer has used. Customer may only use the AWS Marks in accordance with the Trademark Use Guidelines. Customer will not misrepresent or embellish the relationship between AWS and Customer (including by expressing or implying that AWS supports, sponsors, endorses, or contributes to Customer or Customer's business endeavors). Customer will not imply any relationship or affiliation between AWS and Customer except as expressly permitted by this Agreement.

8.5 Suggestions. If Customer elects to provide any Suggestions to AWS or its Affiliates, AWS and its Affiliates will be entitled to use the Suggestions without restriction. Customer hereby irrevocably assigns to AWS all right, title, and interest in and to the Suggestions.

9. Customer Representations, Warranties and Covenants.

9.1 Customer Commitments. Customer represents, warrants and covenants that (i) Customer and any End Users' use of the Service Offerings (including any activities under a Customer Account and use by Customer's employees and personnel), Customer Content and Customer Submissions will not violate this Agreement or applicable law; (ii) Customer Content or Customer Submissions, the combination of Customer Content or Customer Submissions with other applications, content or processes, or the use, development, design, production, advertising or marketing of Customer Content or Customer Submissions, do not and will not infringe or misappropriate any third-party rights; and (iii) Customer's use of the Service Offerings will not cause harm to any End Users.

9.2 Process. AWS will promptly notify Customer of any claim subject to Section 9.1, but if AWS fails to promptly notify Customer, this will only affect Customer's obligations under Section 9.1 to

the extent that AWS's failure prejudices Customer's ability to defend the claim. Customer may: (a) use counsel of its own choosing to defend against any claim; and (b) settle the claim as Customer deems appropriate.

10. AWS Warranties and Warranty Disclaimers.

10.1 AWS Warranties. AWS represents and warrants to Customer that the Services will perform substantially in accordance with the Documentation.

10.2 Warranty Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 10.1 (AWS WARRANTIES) AND SECTION 12 OF THE GENERAL PROVISIONS ("WARRANTY"), THE SERVICE OFFERINGS ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS, ITS AFFILIATES AND ITS LICENSORS MAKE NO OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND DISCLAIM ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (A) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (B) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (C) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, AND (D) THAT ANY CONTENT, INCLUDING CUSTOMER CONTENT OR THIRD-PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

11. Limitations of Liability.

11.1 Liability Disclaimers. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9 (CUSTOMER REPRESENTATIONS, WARRANTIES, AND COVENANTS), NEITHER PARTY NOR ANY OF THEIR AFFILIATES OR LICENSORS WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR (A) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, (B) THE VALUE OF LOST DATA, LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, OR GOODWILL, OR (C) UNAVAILABILITY OF THE SERVICE OFFERINGS (THIS DOES NOT LIMIT ANY SERVICE CREDITS THAT MAY BE AVAILABLE UNDER THE SERVICE LEVEL AGREEMENTS OR TO AWS'S COMMITMENTS UNDER SECTION 10.1).

11.2 Damages Cap. EXCEPT FOR PAYMENT OBLIGATIONS ARISING UNDER SECTION 9 (CUSTOMER REPRESENTATIONS, WARRANTIES, AND COVENANTS), THE AGGREGATE LIABILITY UNDER THIS AGREEMENT OF EITHER PARTY AND ANY OF THEIR RESPECTIVE AFFILIATES OR LICENSORS WILL NOT EXCEED THE LESSER OF (A) THE AMOUNTS PAID BY CUSTOMER TO AWS UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE, OR (B) USD $20,000,000; PROVIDED, HOWEVER THAT NOTHING IN THIS SECTION 11 WILL LIMIT CUSTOMER'S OBLIGATION TO PAY AWS FOR CUSTOMER'S USE OF THE SERVICE OFFERINGS PURSUANT TO SECTION 5, OR ANY OTHER PAYMENT OBLIGATIONS UNDER THIS AGREEMENT.

12. Miscellaneous.

12.1 [RESERVED]

12.2 [RESERVED]

12.3 Entire Agreement. This Agreement incorporates the Policies by reference and is a part of the Contract as Exhibit A. Except to the extent specified in the Contract, AWS will not be bound by any term, condition or other provision which is different from or in addition to the provisions of this Agreement (whether or not it would materially alter this Agreement) including for example, any term, condition or other provision (a) submitted by Customer in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other questionnaire, or (c) related to any invoicing process that Customer submits or requires AWS to complete. If the terms of this document are inconsistent with the terms contained in any Policy, the terms contained in this document will control, except that the Service Terms will control over this document.

12.4 [RESERVED]

12.5 [RESERVED]

12.6 Import and Export Compliance. In connection with this Agreement, each party will comply with all applicable import, re-import, export, and re-export control laws and regulations, including the Export Administration Regulations, the International Traffic in Arms Regulations, and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control. Customer is solely responsible for compliance with applicable laws related to the manner in which Customer chooses to use the Service Offerings, including (i) Customer's transfer and processing of Customer Content, (ii) the provision of Customer Content to End Users, and (iii) specifying the AWS region in which any of the foregoing occur.

12.7 [RESERVED]

12.8 Language. All communications and Notices made or given pursuant to this Agreement must be in the English language. If AWS provides a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

12.9 Nondisclosure. The Mutual Nondisclosure Agreement (NDA) is incorporated by reference into this Agreement, except that the security provisions in Section 3, not the NDA, apply to Customer Content.

12.10 Notice.

(a) General. Except as otherwise set forth in Section 12.10(b), to give notice to a party under this Agreement, each party must contact the other party as follows: (i) by facsimile transmission; or (ii) by personal delivery, overnight courier or registered or certified mail. Notices must be sent to the contract party listed by each Individual Enterprise Account associated with this Agreement or such other contact information as a party may subsequently designate in a notice to the other party. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided by registered or certified mail will be effective three (3) business days after they are sent.

(b) Electronic Notice. AWS may provide notice to Customer: (i) under Sections 2.3 or 5.1 by (A) sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts, or (B) posting a notice on the AWS Site, (ii) under Section 6.1 by sending a message to the email address then associated with Customer's applicable AWS Enterprise Account, and (iii) under Section 2.1 by sending a message to the email address then associated with at least one of Customer's AWS Enterprise Accounts (or such other email address as agreed upon by the parties) or via a support case. Any notices provided by posting on the AWS Site will

be effective upon posting and notices provided by email will be effective when AWS sends the email.

12.11 No Third-Party Beneficiaries. Except as set forth in Section 9.1, this Agreement does not create any third party beneficiary rights in any individual or entity that is not a party to this Agreement.

12.12 No Waivers. The failure by either party to enforce any provision of this Agreement will not constitute a present or future waiver of such provision nor limit such party's right to enforce such provision at a later time. All waivers by a party must be provided in a Notice to be effective.

12.13 [RESERVED]

13. Definitions. Defined terms used in this Agreement with initial letters capitalized have the meanings given below:

"**Acceptable Use Policy**" means the policy currently available at http://aws.amazon.com/aup (and any successor or related locations designated by AWS), as it may be updated by AWS from time to time.

"**Account Information**" means information about Customer that Customer provides to AWS in connection with the creation or administration of an AWS Enterprise Account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with an AWS Enterprise Account.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by or is under common control with that party.

"**API**" means an application program interface.

"**AWS Content**" means Content that AWS or any of its Affiliates makes available in connection with the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; sample code; software libraries; command line tools; proofs of concept, templates, and other related technology (including but not limited to any of the foregoing that are provided by any AWS personnel). AWS Content does not include the Services or Third-Party Content.

"**AWS Customer Agreement**" means AWS's standard user agreement posted on the AWS Site at http://aws.amazon.com/agreement (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**AWS Enterprise Account**" means an AWS account opened by Customer using a Customer-issued email address (with an email domain name that is owned by Customer) that includes Customer's full legal name in the "Company Name" field associated with the AWS account and other designating information as mutually agreed by the parties.

"**AWS Marks**" means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its Affiliates that AWS may make available to Customer in connection with this Agreement.

"**AWS Network**" means 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.

"AWS Security Standards" means the security standards attached to this Agreement as Attachment A.

"**AWS Site**" means http://aws.amazon.com (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Content**" means software (including machine images), data, text, audio, video, or images.

"**Customer Content**" means Content that Customer or any End User transfers to AWS for processing, storage or hosting by the Services in connection with an AWS Enterprise Account and any computational results that Customer or any End User derive from the foregoing through its use of the Services. For example, Customer Content includes Content that Customer or any End User stores in Amazon Simple Storage Service. Customer Content does not include Account Information.

"**Customer Submissions**" means Content that Customer posts or otherwise submits to developer forums, sample code repositories, public data repositories, community-focused areas of the AWS Site, or any other part of the AWS site that allows third parties to make available software, products, or data.

"**Disputed Amounts**" means amounts disputed by Customer in a Notice and in good faith as billing errors.

"**Documentation**" means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by AWS), as such user guides and admin guides may be updated by AWS from time to time.

"**End User**" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Customer Content; or (b) otherwise accesses or uses the Service Offerings under an AWS Enterprise 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 an AWS Enterprise Account.

"**Indirect Taxes**" means applicable taxes and duties, including, without limitation, VAT, GST, excise taxes, sales and transactions taxes, and gross tax receipts.

"**Losses**" means any claims, damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees).

"NDA" means the Mutual Nondisclosure Agreement (NDA) between Customer and Amazon.com, Inc., dated [_____], 20__.

"Notice" means any notice provided in accordance with Section 12.10.

"**Policies**" means the Acceptable Use Policy, Privacy Policy, the Terms of Use, the Service Terms, the Trademark Use Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into this Agreement, but does not include whitepapers or other marketing materials referenced on the AWS Site.

"**Privacy Policy**" means the privacy policy currently referenced at http://aws.amazon.com/privacy (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Service**" means each of the services made available by AWS or its Affiliates for which Customer registers via the AWS Site, including those web services described in the Service Terms. Services do not include Third-Party Content.

"**Service Attributes**" means Service usage data related to an AWS Enterprise Account, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics.

"**Service Level Agreement**" means all service level agreements that AWS offers with respect to the Services and post on the AWS Site, as they may be updated by AWS from time to time. The

service level agreements that AWS currently offers with respect to the Services are located at https://aws.amazon.com/legal/service-level-agreements (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Service Offerings**" means the Services, the AWS Content, the AWS Marks, and any other product or service provided by AWS under this Agreement. Service Offerings do not include Third-Party Content.

"**Service Terms**" means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Suggestions**" means all suggested improvements to the Service Offerings that Customer provides to AWS.

"**Term**" means the term of this Agreement described in Section 7.1.

"Termination Date" means the effective date of termination provided in accordance with Section 7, in a Notice from one party to the other.

"**Terms of Use**" means the terms of use located at http://aws.amazon.com/terms/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

"**Third-Party Content**" means Content of a third party made available on the AWS Marketplace or on developer forums, sample code repositories, public data repositories, community-focused areas of the AWS Site, or any other part of the AWS site that allows third parties to make available software, products, or data.

"**Trademark Use Guidelines**" means the guidelines and trademark license located at http://aws.amazon.com/trademark-guidelines/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

EXHIBIT H
AWS Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable AWS Service Agreement.

1. **Information Security Program.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) 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:

   1.1 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.

   1.2 Physical Security

   1.2.1 Physical Access Controls. 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 (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). 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.

   1.2.2 Limited Employee and Contractor Access. 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.

   1.2.3 Physical Security Protections. 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 (e.g., primary entry doors, emergency egress

doors, roof hatches, dock bay doors, etc.) 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.

2. **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. **Security Breach Notification.** If AWS has actual knowledge of the unauthorized access to or acquisition of any record containing Customer Content that is subject to applicable data breach notification law and such access or acquisition is caused by a confirmed breach of the security measures described in these AWS Security Standards that renders misuse of the information reasonably likely, AWS will (a) promptly notify Customer, as required by applicable law, and (b) take commercially reasonable measures to address the breach in a timely manner."

EXHIBIT I
Mutual Nondisclosure Agreement

CC NDA 00339477 2022 TR

MUTUAL NONDISCLOSURE AGREEMENT

The parties have executed this Agreement as of the Effective Date.

Amazon Web Services, Inc.	**California Department of Technology**
By: _____.	By: _____.
its _____	its _____
Print Name: _____	Print Name: _____
Date Signed: _____	Date Signed: _____
Courier: 410 Terry Ave. N., Seattle, WA 98109-5210 Mail: P.O. Box 81226, Seattle, WA 98108-1226 Email: contracts-legal@amazon.com Attention: General Counsel	Mail: 10860 Gold Camp Drive, Rancho Cordova, CA 95670 - United States Email: Danielle.Kanelos@state.ca.gov Attention: Danielle Kanelos

This Mutual Nondisclosure Agreement (this "Agreement"), effective as of May 13, 2022 (the "Effective Date"), is made between Amazon Web Services, Inc., a Delaware corporation ("Amazon"), and California Department of Technology, a California public entity ("Company"). In connection with the parties' commercial relationship or discussions about a possible relationship or transaction (the "Relationship"), each party may receive confidential information from the other party. Accordingly, Amazon and Company hereby agree as follows:

1. **Affiliates; Confidential Information.** The term "Affiliate" means, with respect to either party, any entity that directly or indirectly controls, is controlled by or is under common control with that party, and the term "Confidential Information" means all nonpublic information concerning the Relationship disclosed by either party, its Affiliates, or their agents (as applicable, such entities collectively, the "Disclosing Party") to the other party, its Affiliates, or their agents (collectively, the "Receiving Party") that is designated as confidential or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered as confidential. Confidential Information includes, without limitation (i) nonpublic information relating to the Disclosing Party's technology, products, services, processes, data, customers, business plans and methods, promotional and marketing activities, finances and other business affairs, (ii) third-party information that the Disclosing Party is obligated to keep confidential, and (iii) subject to the California Public Records Act, the nature, content and existence of a Relationship, discussions or negotiations between the parties.

2. **Exclusions.** Confidential Information does not include any information that (i) is or becomes publicly available without breach of this Agreement (provided, however, information that is rumored or reported does not become public based only on such rumors or reports), (ii) was known by the Receiving Party prior to its receipt from the Disclosing Party, (iii) is disclosed to the Receiving Party from any third party, except where the Receiving Party knows, or reasonably should know, that such disclosure constitutes a wrongful or tortious act or (iv) is independently developed by the Receiving Party without use of any Confidential Information.

3. **Use and Disclosure of Confidential Information.** The Receiving Party will use Confidential Information only in connection with the Relationship. Except as provided in this Agreement or to the extent provided by applicable law, the Receiving Party will not disclose Confidential Information to anyone without the Disclosing Party's prior written consent. The Receiving Party will take reasonable measures to avoid disclosure, dissemination or unauthorized use of Confidential

Information. If a request for Confidential Information is made under the California Public Records Act or applicable law, Company will provide Amazon.com with reasonable advance written notice to permit Amazon.com to seek a protective order or other appropriate remedy to prevent the disclosure of such information to the maximum extent permitted under applicable law.

4. **Receiving Party Personnel; Affiliates.** The Receiving Party will restrict the possession, knowledge and use of Confidential Information to its directors, officers, employees, contractors, agents, legal and accounting advisers, and entities controlled by the Receiving Party (collectively, "Personnel") who (i) have a need to know Confidential Information in connection with the Relationship, (ii) are informed of the confidential nature of the Confidential Information, and (iii) have obligations with respect to the Confidential Information that are consistent with this Agreement. Each of Amazon and the Company will ensure that its Affiliates comply with this Agreement.

5. **Disclosures to Governmental Entities.** The Receiving Party may disclose Confidential Information as required to comply with orders of governmental entities that have jurisdiction over it or as otherwise required by law.

6. **Ownership of Confidential Information.** All Confidential Information will remain the exclusive property of the Disclosing Party. The Disclosing Party's disclosure of Confidential Information will not constitute an express or implied grant to the Receiving Party of any rights to or under the Disclosing Party's patents, copyrights, trade secrets, trademarks or other intellectual property rights. Except to the extent permitted by applicable law in the absence of any express license or other grant of rights, neither party will use any trade name, trademark, logo or any other proprietary rights of the other party (or any of its Affiliates) in any manner without prior written authorization of such use by a Vice President of such other party.

7. **Notice of Unauthorized Use.** The Receiving Party will notify the Disclosing Party promptly upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this Agreement by the Receiving Party. The Receiving Party will cooperate with the Disclosing Party to help the Disclosing Party regain possession of such Confidential Information and prevent its further unauthorized use and disclosure.

8. **Return of Confidential Information.** Subject to compliance with orders of governmental entities that have jurisdiction over it or as otherwise required by law, the Receiving Party will return or destroy all tangible materials or portions thereof constituting Confidential Information (including, without limitation, all summaries, copies and excerpts of Confidential Information) promptly following the Disclosing Party's written request.

9. **Injunctive Relief.** The Receiving Party acknowledges that a breach of its obligations under this Agreement could cause irreparable harm to the Disclosing Party as to which monetary damages may be difficult to ascertain or an inadequate remedy. The Receiving Party therefore agrees that the Disclosing Party will have the right, in addition to its other rights and remedies, to seek injunctive relief for any violation of this Agreement.

10. **Scope; Termination.** This Agreement covers Confidential Information disclosed by the Disclosing Party on and after the Effective Date. This Agreement automatically will terminate upon the earlier of (i) termination of all written agreements between the parties or their Affiliates regarding the Relationship, or (ii) if no agreements are executed, termination of discussions between the parties or their Affiliates regarding the Relationship or delivery of written notice terminating this Agreement; provided, however, that (a) each party's obligations with respect to the other party's Confidential Information will survive for three (3) years following termination, and (b) Sections 6, 9, 10, and 11 will survive indefinitely.

11. **Miscellaneous.**

11.1 This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes all prior communications and agreements between the parties with respect thereto. This Agreement may be amended, modified, or waived only with the mutual written consent of the parties hereto. This Agreement will not be assignable by either party without the prior written consent of the other party; provided that prior written consent will not be required for any assignment by a party to an Affiliate. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties and their respective successors and assigns.

11.2 The Disclosing Party acknowledges that the Receiving Party may now have, or in the future may develop or receive, information that is the same as, or

similar to, Confidential Information without having breached this Agreement. Nothing in this Agreement (a) prevents the Receiving Party from using, for any purpose and without compensating the Disclosing Party, information retained in the memory of the Receiving Party's Personnel who have had access to Confidential Information or (b) obligates the Receiving Party to restrict the scope of employment of the Receiving Party's Personnel provided, however, that this section does not create a license under any copyright or patent of the Disclosing Party.

11.3 If a provision of this Agreement is held invalid under any applicable law, such invalidity will not affect any other provision of this Agreement that can be given effect without the invalid provision. Further, all terms and conditions of this Agreement will be deemed enforceable to the fullest extent permissible under applicable law, and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.

11.4 This Agreement will be governed by internal laws of the State of California, without reference to its choice of law rules. Exclusive jurisdiction over and venue of any suit arising out of or relating to this Agreement will be in the state and federal courts located in Sacramento County, California, and each of the parties hereto consents to the personal jurisdiction of, and venue in, those courts.

11.5 All notices hereunder will be given in writing, will refer to this Agreement and will be personally delivered or sent by overnight courier, electronic mail, or registered or certified mail (return receipt requested) to the address set forth below the parties' signatures on the first page of this Agreement.