SCO ID:

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-14308	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

Mythics, 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:

$500,000.00 - Five Hundred Thousand 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	9
	Exhibit A-1	Service Level Agreements (SLAs)	1
	Exhibit B	Payment and Invoicing	2
+ -	Exhibit C	Cost Proposal Worksheet	1
+ -	Exhibit D	FedRAMP High Cloud Computing General Provisions - Information Technology	18
+ -	Exhibit E	FedRAMP High Cloud Computing Services Special Provisions	5
+ -	Exhibit F	Oracle Public Sector Cloud Services Agreement Terms	10
+ -	Exhibit G	Data Processing Agreement for Oracle Services	5
+ -		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.)

Mythics, Inc.

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
4525 Main Street, Ste 1500	Virginia Beach	VA	23462

PRINTED NAME OF PERSON SIGNING	TITLE
Deonte J. Watters	Vice President of Contracts

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
Deonte J. Watters	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)
20-14308	CDT-7502

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME			
California Department of Technology			
CONTRACTING AGENCY ADDRESS	**CITY**	**STATE**	**ZIP**
10860 Gold Center Drive	Rancho Corodova	CA	95670
PRINTED NAME OF PERSON SIGNING	**TITLE**		
Kristine VanKeuren	Software Services Supervisor		
CONTRACTING AGENCY AUTHORIZED SIGNATURE	**DATE SIGNED**		
Kristine VanKeuren (May 17, 2022 11:57 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

The Mythics, 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 High 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 their Cloud Service Provider's 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 place 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 all entities. 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 is incorporated by reference into this Agreement as if attached hereto.

4. Data/Information Categorization:

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

5. 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		Oracle	
Attn:	Scott MacDonald	Attn:	Abhijeet Dabke
Phone:	(916) 228-6460	Phone:	(916) 803-3240
E-mail:	Scott.MacDonald@state.ca.gov	Web:	Abhijeet.V.Dabke@oracle.com

Contract inquiries should be addressed to:

State Agency		Contractor	
CDT, Acquisitions & IT Program Management Branch		Mythics, Inc.	
Attn:	Jamie Wong	Attn:	Eric Dunnet
Address:	PO Box 1810 Rancho Cordova, CA 95741	Address:	4525 Main Street. Ste 1500 Virginia Beach, VA 23462
Phone:	(916) 431- 4105	Phone:	(856) 308-0886
E-mail:	Jamie.Wong@state.ca.gov	E-mail:	edunnet@mythics.com

6. Technical Requirements

a. The CSP's cloud services offered hereunder must be FedRAMP Authorized at the High level, as proposed.
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 CSP's 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. See also, SOW Section 14. Clarifications to General and Special Provisions.
e. The CSP must provide the state with the root access to the master payer account.

Application Programming Interface Requirements (Mandatory)

The Contractor's 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 (Mandatory)

The Contractor's 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.

7. Reserved Instances (Not Mandatory)

Reserved Instances may be available for use on this Agreement.

8. 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 the FedRAMP High Cloud Computing General Provisions - Information Technology-Exhibit D.
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.

9. 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).

10. 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.

11. 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: Eric Dunnet, (856) 308-0886, eddunet@mythics.com
Second Level: Ryan Williams, (757) 506-6306, rwilliams@mythics.com
Third Level: Eric Seifert, (757) 374-0856, eseifert@mythics.com

12. 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.

13. Cancellation Provisions

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

14. Clarifications and Revisions to General and Special Provisions

Section 1.z.ii (State Data) of the General Provisions will be clarified by the following:

"Unless otherwise specified in the Service Specifications, Oracle's Services can only accept, and you will only provide, personal data which does not have data protection, security controls or regulatory requirements (e.g., Oracle Payment Card Industry (PCI)) that are in addition to those applicable to personally identifiable information.

If available, a User may purchase Services (e.g., Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services, etc.) designed to address particular data protection requirements. The applicable Service Specifications will identify whether the Services are designed to address data protection requirements applicable to PCI and/or Protected Health Information (PHI) and/or other types of protected data.

Additionally, upon a User's written request, the CSP will identify if the Services a User is requesting to purchase are designed to address data protection requirements applicable to PCI and/ or PHI and/or other types of protected data."

Section 7 (Compliance with Statutes and Regulations) of the General Provisions will be clarified by the following:

The extent to which an Oracle product on the Statement of Work is, prior to any customizations, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), effective as of June, 2001 or the Revised version in Appendix A (known as "Revised Section 508") effective as of January, 2018, and the Web Content Accessibility Guidelines (WCAG) version 2.0 level AA, is indicated by the dependencies, comments and exceptions (some of which may be significant, if any) noted on the applicable Voluntary Product Accessibility Templates (VPAT) available at www.oracle.com/accessibility for each product, when used in accordance with Oracle's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no VPAT is available for a particular Oracle product, please contact the Oracle Accessibility Program Office at accessible_ww@oracle.com. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. No other terms, conditions, statements or any other such representations regarding or related to accessibility shall apply to the Oracle products provided under the Statement of Work. Oracle cannot make any commitments about future product directions, including plans to address

accessibility or the availability of VPATs. Product direction remains at the sole discretion of Oracle.

Section 25 (Contract Modification) of the General Provisions will be clarified by the following:

The parties agree and understand that Attachment 7, Data Processing Agreement for Oracle Services shall remain static for the duration of the contract term plus two (2) option 2-year extensions.

Section 26 (Confidentiality of Data) of the General Provisions will be clarified by the following:

"The parties acknowledge information transmitted by the State to the Contractor and/or Service Provider may inadvertently contain Federal Tax Information (FTI). The State will use all reasonable efforts to prevent the transmittal of FTI to Contractor and/or Service Provider under this Contract. The State further acknowledges that the Contractor and/or Service Provider does not require any “access” to, or “receipt” or “storage” of FTI to perform the Services under the Contract. The Contractor and/or Service Provider further acknowledges that Contractor and/or Service Provider shall not knowingly access or permit access to such FTI, unless directed by the State. Access to FTI is out-of-scope of the Services. To the extent that Contractor’s and/or Service Provider’s access to FTI is “incidental” to Contractor’s provision of Services, it is the parties’ view that such incidental exposure should not legally subject Contractor and/or Service Provider to the Internal Revenue Service (IRS) requirements set forth in IRS Publication 1075, section 11.2. If, however, the IRS ultimately takes a contrary position, and determines that Contractor, Service Provider and/or the State should have nevertheless complied with the requirements of IRS Publication 1075, the parties will immediately commence an evaluation of the feasibility of continued performance under the Contract."

Section 3 (Data Protection) of the Special Provisions will be clarified by the following:

Subsection 3.a:

The Service Provider states that it has adopted security controls and practices for its Services designed to protect the confidentiality, integrity, and availability of State Data hosted by the Service Provider in the Services. The Service Provider continually works to strengthen and improve those security controls and practices. To this end, the Service Provider shall safeguard the confidentiality and integrity of State Data within its control and comply, in lieu of Sections 3, introductory paragraphs and 3.a (i–iii), with all laws expressly applicable to it as a data processor or information technology services provider for the provisioning of the Service(s).

Subsection 3.b:

As between the Service Provider and the State, all State Data shall become and remain the property of the State. The Service Provider may compile statistical and other information as set forth in Section 10 (Service Monitoring, Analyses and Oracle Software) of the Oracle Cloud Services Agreement Terms; however, Services Analyses will not incorporate State Data in a form that could serve to identify the State or any individual and do not constitute State Data.

Subsection 3.c:

Personal Data and Non-Public Data shall be encrypted at rest, in use, and/or in transit with controlled access only if expressly ordered by the Customer and as set forth elsewhere in a SOW created for the transaction. Unless expressly stated otherwise elsewhere in such SOW, the State is responsible for encryption of and access control to the State Data for the service model under contract.

Subsection 3.d:

As between the Service Provider and the State, all State Data shall become and remain the property of the State. The Service Provider may compile statistical and other information as set forth in Section 10 (Service Monitoring, Analyses and Oracle Software) of the Oracle Cloud Services Agreement Terms; however, Services Analyses will not incorporate State Data in a form that could serve to identify the State or any individual and do not constitute State Data.

Section 7 (Data Preservation and Retrieval) of the Special Provisions will be clarified by the following:

After termination of the Contract and the prescribed retention period, the Service Provider shall securely dispose of all State Data in all forms. State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. At the State's written request, once and upon termination, the Service Provider will provide the State with a confirmation that the State's Content in the Services environment has been deleted or rendered inaccessible.

Section 8 (Background Checks) of the Special Provisions will be clarified by the following:

Oracle, or its agent, has performed a background check on Oracle employees hired on or after January 1, 2003 in the United States. As of this date, the background check is used to attempt to: (i) ascertain an employee's previous employment with up to three (3) employers within the five (5) years preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Oracle. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Oracle." Where allowable under applicable law, Oracle has established similar pre-employment background screening procedures in regions outside of the United States, subject to local laws, regulations, and customs.

Section 9 (Access to Security Logs and Reports) of the Special Provisions will be clarified by the following:

The parties agree and understand that Oracle Audit is a web service that automatically records calls to public application programming interface (API) endpoints for the State's Oracle Cloud Infrastructure. The service creates audit log events for each call that can be viewed, retrieved, stored, and analyzed. The log events include information such as the ID of the caller, the target resource, the time of the recorded event, request parameters, and response parameters. The State can access log events using the API, the Console, and the Java Software Development Kit (SDK). The Service Provider will provide the log events upon written request. The delineation of specific shared responsibilities, between the Service Provider and the State, are set forth in the Service Specifications (as defined in the Oracle Cloud Services Agreement Terms).

To review FAQs about the Oracle Cloud Infrastructure Audit, please see https://cloud.oracle.com/governance/audit/faq.

Section 10 (Contract Audit) of the Special Provisions will be clarified by the following:

The State's audit rights are further clarified in the Data Processing Agreement for Oracle Services.

Section 15 (Responsibilities and Uptime Guarantee) of the Special Provisions will be clarified by the following:

The Service Specifications for the relevant cloud service (as defined in Section 17.3 of the Oracle Cloud Services Agreement Terms) detail the availability and performance of the particular environments.

Section 17 (Business Continuity and Disaster Recovery) of the Special Provisions will be clarified by the following:

Pursuant to the Oracle Hosting and Delivery Policies and the applicable Pillar Documents, the State is responsible for developing its own business continuity plan.

15. 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.

EXHIBIT A-1
SERVICE LEVEL AGREEMENTS (SLAs)

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

a) Service Credits

1) The state reserves the right to take 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 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 the FedRAMP High 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 High.

Contract Line Item # (CLIN)	Item Description	Contract Discount
1	Infrastructure as a Service for FedRAMP High	8.00%

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

Item Description	Published List Price	Discount Level	Contract Discount %	Contract $
Platform as a Service	$250,000	Base	8%	$ 230,000.00
	$250,000	A	8%	$ 230,000.00
	$250,000	B	8%	$ 230,000.00
	$250,000	C	8%	$ 230,000.00
	$1,000,000		**Evaluated Total:**	$ 920,000.00

(link to catalog)	https://www.mythics.com/cdt2

EXHIBIT D
FEDRAMP HIGH CLOUD COMPUTING GENERAL PROVISIONS – INFORMATION TECHNOLOGY

1. **DEFINITIONS**: Unless otherwise specified in the Statement of Work, the following terms shall be giventhe meaning shown, 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, butthey 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, orother 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 High authorization providing either IaaS or PaaS solicited through the RFP.

   e. **"Contract"** means this Contract or agreement (including any purchase order), by whatever nameknown 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" or other similar term.

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

   h. **"Deliverables"** means the Products and Services other than 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 manuals and other published materials necessary or useful to the State in its use or maintenance of the Products and Services provided hereunder and includes online materials, virtual help, and help desk where available. In addition, manuals and other published materials customized for the State hereunder constitute Work Product.

   j. **"Eligible Public Entity"** means each of the California public entities authorized to purchase the Deliverables and service 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 "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 the state, "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 High"** 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 interactions 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 RFP 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. "**Special Provisions**" means the FedRAMP High Cloud Computing Services Special

Provisions incorporated into this Contract.

y. **"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.

z. **"State Data" (or "Your Content")** 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.

aa. **"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.

bb. **"Subcontract"** means a contract awarded by Contractor to a Subcontractor requiring the Subcontractor to perform Services for the State on the Contractor's behalf, specifically required by and in connection with the Contract.

cc. **"Subcontractor"** means a business entity holding a Subcontract with Contractor. Subcontractors shall not include suppliers that support Contractor's Services not specifically inconnection with this Contract.

dd. **"User" (see also "Customer")** means and 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.

ee. **"U.S. Intellectual Property Rights"** means intellectual property rights enforceable in the UnitedStates 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 toChapters 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 nofurther 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 theperformance 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 warrant 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 applicable to protection of data or Personally Identifiable information as defined in the National Institute of Standards and Technology Special Publication 800-122 or any successor Publication, and all statues applicable to it as a corporation. The Contractor agrees to defend the State against any loss, cost, damage or liability by reason of the Contractor's violation of this provision:

   b. The State will notify the Contractor of any such claim in writing and tender the defense thereof within reasonable time;

   c. The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) 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); (ii) 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 (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations;

   d. 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). This provision applies only to the Reseller; and

   e. To the extent that this Contract falls within the scope of Government Code Section 11135, the Reseller will be responsible to respond to and resolve any complaint brought to its attention, regarding accessibility of its products or services. The State shall designate an authorized representative who will be responsible for submission to Reseller of complaints received by the State regarding the accessibility of Contractor's products. Reseller shall be responsible to review and respond to all complaints regarding accessibility brought to the attention of the State. The State and Reseller shall work together to determine a reasonable response and resolution of all complaints. The State acknowledges that Reseller can satisfy its duty to respond to and resolve complaints under this provision by taking action it deems appropriate under the circumstances, which may in some instances include no further action beyond responding to the complaint.

8. **CONTRACTOR'S POWER AND AUTHORITY:** The Contractor warrants that it has full power

and authority to grant the rights herein granted and will reimburse the State for any loss, cost, liability, and expense (including reasonable attorney fees) arising out of any breach of this warranty. 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.

a. The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and

b. The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) 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); (ii) 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 (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.

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 either party or the failure of either party on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by that party of its rights hereunder and shall not prevent that party from enforcing such provision or right on any future occasion. The rights and remedies of the parties herein are cumulative and are in addition to any other rights or remedies that the parties 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 High 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 High Cloud Computing Special Provisions - Infrastructure as a Service and Platform as a Service (hereafter referred to as, the "Special Provisions");

    d. Cost worksheets; and

    e. The CSP's service agreement and attachments;

    f. All other attachments incorporated in the Contract by reference.

12. WARRANTY:

a. Limited Warranty for Services. In addition to warranties set forth in the agreement, Contractor warrants that:

i. Services will perform 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 Public 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: Service Credits and Performance Discounts as applicable;

i. Service Credits and Performance Discounts as applicable;

ii. Re-performance, repair or refund. In the event the Contractor fails to re-perform or repair the products and/or services as appropriate, the State may end the deficient services and the Contractor shall refund the fees paid for the deficient services for the period of time during which the services were deficient, 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 may be specifically provided elsewhere in this Contract.

d. **DISCLAIMER OF OTHER WARRANTIES.** OTHER THAN THIS LIMITED WARRANTY, CONTRACTOR PROVIDES NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS. CONTRACTOR DISCLAIMS ANY IMPLIED REPRESENTATIONS,

WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OF MERCHANTABILITY, 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 in the Statement of Work:

i. The Contractor does not warrant that any Software provided hereunder is error-free or that it will runwithout immaterial interruption.

ii. The Contractor does not warrant and will have no responsibility for a claim to the extent that it arisesdirectly 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.

13. SUBSTITUTIONS: RESERVED

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 and accident 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;

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

g. 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 or 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. RIGHTS AND REMEDIES OF STATE FOR DEFAULT:

a. In the event of the termination of the Contract, either in whole or in part, by reason of default or breach by the Contractor, any loss or damage sustained by the State in procuring any items which the Contractor agreed to supply shall be borne and paid for by the Contractor (but subject to the clause entitled "Limitation of Liability"); and

b. The State reserves the right to offset the reasonable cost of all damages caused to the State against any outstanding invoices or amounts owed to the Contractor or to make a claim against the Contractor therefore.

20. LIMITATION OF LIABILITY:

a. Contractor's liability for damages to the State for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to which is defined as the then current sum of the amounts paid in aggregate by all State entities for all Services purchased in the twelve month period immediately preceding the event giving rise to such liability ("Collective Aggregate Purchase Value");

b. The foregoing limitation of liability shall not apply (i) to any liability under provisions herein entitled "Compliance with Statutes and Regulations" (ii) to liability under provisions herein entitled "Patent, Copyright, and Trade Secret Indemnity" or to any other liability (including without limitation indemnification obligations) for infringement of third party intellectual property rights; (iii) to claims arising under provisions herein calling for indemnification for third party claims against the State for death, bodily injury to persons or damage to real or tangible personal property caused by the Contractor's negligence or willful misconduct; or (iv) to costs or attorney's fees that the State becomes entitled to recover as a prevailing party in any action;

c. The State's liability for damages for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to the Collective Aggregate Purchase Value, as that term is defined in subsection a) above. Nothing herein shall be construed to waive or limit the State's sovereign immunity or any other immunity from suit provided by law; and

d. 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, EXCEPT (I) TO THE EXTENT THAT THE CONTRACTOR'S LIABILITY FOR SUCH DAMAGES IS SPECIFICALLY SET FORTH IN THE STATEMENT OF WORK OR (II) TO THE EXTENT THAT THE CONTRACTOR'S LIABILITY FOR SUCH DAMAGES ARISES OUT OF SUB SECTION B) (I), B)(II), OR B)(IV) ABOVE.

21. INDEMNIFICATION:
The Contractor agrees to indemnify, defend and save harmless the State, its officers, agents and employees from any and all third party claims, costs (including without limitation reasonable attorneys' fees), and losses due to the injury or death of any individual, or the loss or damage to any real or tangible personal property, resulting from the willful misconduct or negligent acts or omissions of the Contractor or any of its affiliates, agents, subcontractors, employees, suppliers, or laborers furnishing or supplying work, services, materials, or supplies in connection with the performance of this Contract. Such defense and payment will be conditional upon the following:

a. The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and

b. The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) 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); (ii) 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 (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations

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 Contractor 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 State agencies to pay properly submitted, undisputed invoices not more than 45days 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 attorneys' 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 this Section will be conditional upon the following:

i. The State will notify the Contractor of any such claim in writing and tender the defense thereof 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 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 Technology 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. immediately 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 shall be prevented by injunction, 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 the 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 rights caused solely by the Services, and shall have no liability to the State under anyprovision of this clause with respect to any claim of patent, copyright or trade secret infringement which is based upon:

   i. The modification initiated by the State, User, or a third party at the State's direction, of any Service furnished hereunder;
   ii. The combination or utilization of Software furnished hereunder with non-contractor supplied Software;
   iii. Any use of the Services, or any other act, that is in breach of this Agreement;
   iv. Any use of the Services, or any other act by the State or Users, that is in breach of this Agreement;
   v. Any claim of inducement or contributory negligence;
   vi. Any claim of willful infringement directed at anyone other than the Contractor or the CSP; or
   vii. Any use of the Services after the CSP has notified the State or Users to discontinue such use.

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 allow the auditor(s) access to such records during normal business activities and to allow interviews of any employees or others who might reasonably have information related to such records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Contract. The State shall provide reasonable advance written notice of such audit(s) to the Contactor.

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.

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.

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 asif 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 work under the Contract.

35. **NATIONAL LABOR RELATIONS BOARD CERTIFICATION:** The Contractor swears under penaltyof 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.

    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 costsincurred 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 injuredby 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 informemployees 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 theContract.

38. FOUR-DIGIT DATE COMPLIANCE: Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Deliverables and/or services to the State. "Four Digit Date Compliant" Deliverables and 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. SWEATFREE CODE OF CONDUCT:

a. Contractor declares under penalty of perjury that no equipment, materials, or supplies furnished to the State pursuant to the Contract have been produced in whole or in part by sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor, or with the benefit of sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. The Contractor further declares under penalty of perjury that they adhere to the Sweatfree Code of Conduct as set forth on the California Department of Industrial Relations website located at www.dir.ca.gov, and Public Contract Code Section 6108; and

b. The Contractor agrees to cooperate fully in providing reasonable access to its records, documents, agents or employees, or premises if reasonably required by authorized officials of the State, the Department of Industrial Relations, or the Department of Justice to determine the Contractor's compliance with the requirements under paragraph (a).

40. RECYCLED CONTENT REQUIREMENTS: The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material (as defined in the Public Contract Code (PCC) Section 12200-12209), in products, materials, goods, or supplies offered or sold to the State that fall under any of the statutory categories regardless of whether the product meets the requirements of Section 12209. The certification shall be provided by the contractor, even if the product or good contains no postconsumer recycled material, and even if the postconsumer content is unknown. With respect to printer or duplication cartridges that comply with the requirements of Section12156(e), the certification required by this subdivision shall specify that the cartridges so comply (PCC 12205 (b)(2)). A state agency contracting officer may waive the certification requirements if the percentage of postconsumer material in the products, materials, goods, or supplies can be verified in a written advertisement, including, but not limited to, a product label, a catalog, or a manufacturer or vendor Internet web site. Contractors are to use, to the maximum extent economically feasible in the performance of the contract work, recycled content products (PCC 12203(d)).

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 complywith 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 ofall employees and is providing the names of all new employees to the New Hire Registry maintained bythe 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. **ELECTRONIC WASTE RECYCLING ACT OF 2003:** The Contractor certifies that it complies with the applicable requirements of the Electronic Waste Recycling Act of 2003, Chapter 8.5, Part 3 of Division 30, commencing with Section 42460 of the Public Resources Code. The Contractor shall maintain documentation and provide reasonable access to its records and documents that evidence compliance.

44. **USE TAX COLLECTION:** In accordance with PCC Section 10295.1, the Contractor certifies that it complies with the requirements of Section 7101 of the Revenue and Taxation Code. Contractor further certifies that it will immediately advise the State of any change in its retailer's seller's permit or certification of registration or applicable affiliate's seller's permit or certificate of registration as described in subdivision (a) of PCC Section 10295.1.

45. **EXPATRIATE CORPORATIONS:** Contractor hereby declares that it is not an expatriate corporation or subsidiary of an 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 theContractor 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 E
FEDRAMP HIGH CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

Infrastructure as a Service and Platform as a Service

These FedRAMP High Cloud Computing Special Provisions (Infrastructure as a Service and Platform as a Service) ("FedRAMP High Cloud Special Provisions) Shall apply to all Eligible Public 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 HIGH 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/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. **DEFINITIONS:** Capitalized terms not defined below shall have the same meaning set forth in the General Provisions.

   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 an unlawful access, use, theft or destruction to any State Data stored in 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) **"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 that unless 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.

   d) **"State Identified Contract"** means the person or persons designated in writing by the State to receive a 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:**

a) In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions, the Service Provider shall comply as required with:

(i) The California Information Practices Act (Civil Code Sections 1798 et seq);

(ii) NIST Special Publication 800-53 Revision 4 or its successor; and

(iii) Privacy provisions of the Federal Privacy Act of 1974.

b) 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.

c) Unless otherwise provided, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made part of this Contract.

d) At no time shall any Personal Data and Non-Public 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 permitted.

e) The State and Eligible Public Entities shall enter into and comply with the applicable provisions of the Health Insurance Portability and Accountability Act of 1996 when using the services to store or transmit any Protected Health Information.

c) **(For PaaS Only)** Encryption of Data at Rest: The Service Provider shall make available storage encryption consistent with validated cryptography standards in accordance with applicable FIPS 140-2 (or its successor) standards as referenced in FedRAMP.

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 located solely 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. **DATA BREACH NOTIFICATION:**

Subject to the requirement to register administrator contact information, as set forth in the following paragraph, if the CSP becomes aware of a Data Breach the CSP will immediately

investigate the Data Breach, and as soon as possible and no later than seventy-two (72) hours after the service provider determines that a Data Breach has occurred: (1) notify one or more State Identified Contacts of the Data Breach; (2) provide the State with detailed information about the Data Breach; and(3) take commercially reasonable measures to mitigate the effects and to minimize any damage resulting from the Data Breach. The CSP and Contractor shall reasonably cooperate fully with the State, its agents and law enforcement in investigating any such data breach.

Notification(s) of Data Breach 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 Data Breach under this section is not an acknowledgement by the service provider of any fault or liability with respect to the Data Breach. The State must notify the CSP promptly about any possible misuse of its accounts or authentication credentials or any Data Breach related to an Online Service.

Data Breach Response Process:

- CSP shall maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

- CSP shall track, or enable the State or Users to track, disclosures of State Data, including what data has been disclosed, to whom, and at what time.

- Service Monitoring: CSP's security personnel verify logs at least every six months to propose remediation efforts if necessary. It is acknowledged that the CSP will provide log data that is related to the State contract only. **[TERM ADDED to proposed Oracle FedRAMP High SPs]**

6. NOTIFICATION OF LEGAL REQUESTS:

Service Provider shall not respond to legal requests directed at the State or Eligible Public Entities 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 relevant Eligible Public Entity within a reasonable time before disclosing State Data in response to any electronic discovery, litigation holds, discovery searches and expert testimonies directed at the Service Provider requesting that the Service Provider disclose State Data under this Contract.

Except as 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 used to 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 data retrieval 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 Data shall 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 and not provide access to State Data to any persons who fail such background checks, in accordance with the requirements of FedRAMP (High 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 available to 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.

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 even 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 or Eligible Public Entity receives a California Public Records Act request for the audit report, the State or Eligible Public Entity shall provide the Service Provider reasonable written notice to enable the Service Provider to take steps to prevent the disclosure of such information to the maximum extent permitted by law.

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 it makes generally 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 to import 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. REMOVAL OF INDIVIDUALS:

The State shall have the right at any time to request that 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 the Service 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 disaster recovery program as it pertains to the Services.

18. WEB SERVICES:

The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible, or as mutually agreed in the SOW and/or SLA.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

EXHIBIT F
ORACLE PUBLIC SECTOR CLOUD SERVICES AGREEMENT TERMS

THESE ORACLE CLOUD SERVICES AGREEMENT TERMS APPLY TO THE ORACLE CLOUD SERVICES THAT YOU ORDER. THESE ORACLE CLOUD SERVICES AGREEMENT TERMS SHALL TAKE PRECEDENCE OVER ANY CONFLICTING TERMS IN AN ORDER OR ANY ORDERING DOCUMENTATION.

1. USE OF THE SERVICES

1.1 Oracle will make the Oracle services listed in Your order (the "Services") available to You pursuant to this Agreement and Your order. Except as otherwise stated in this Agreement or Your order, You have the non- exclusive, worldwide, limited right to use the Services during the period defined in Your order, unless earlier terminated in accordance with this Agreement or the order (the "Services Period"),solely for the internal business operations of the applicable User. You may allow Your Users to use the Services for this purpose, and You are responsible for their compliance with this Agreement and Your order.

1.2 The Service Specifications describe and govern the Services. During the Services Period, Oracle may update the Services and Service Specifications to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of system use, and availability of Third Party Content. Oracle updates to the Services or Service Specifications will not materially reduce the level of performance, functionality, security or availability of the Services during the Services Period of Your order.

1.3 You may not, and may not cause or permit others to: (a) use the Services to harass any person; cause damage or injury to any person or property; publish any material that is false, defamatory, harassing or obscene; violate privacy rights; promote bigotry, racism, hatred or harm; send unsolicited bulk e-mail, junk mail, spam or chain letters; infringe property rights; or otherwise violate applicable laws, ordinances or regulations; (b) perform or disclose any benchmarking, availability or performance testing of the Services, without Oracle's prior written permission. For purposes of the preceding sentence, the reference to "benchmarking" refers to any assessment, measurement or testing of the functionality, security, performance or workload capacity of the Services, including any software or hardware components thereof; or (c) perform or disclose network discovery, port and service identification, vulnerability scanning, password cracking, remote access or penetration tests of the Services (the "Acceptable Use Policy").

With respect to the Oracle PaaS and IaaS Cloud Services acquired under this agreement, the Oracle Cloud Security Testing Policy describes when and how Users may run vulnerability and penetration tests of specified components that they manage through or introduce into the applicable Services. A copy of the Oracle Cloud Security Testing Policy may be accessed at https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/oracle-cloud-security-testing-policy.html#GUID-7238434F-6541-4FF7-9E79-E90A48631413, and is part of the Program Documentation included in Your Service Specifications for the applicable Oracle PaaS and IaaS Cloud Services. Nothing in this section will be deemed to permit any penetration or vulnerability testing of any Oracle SaaS Cloud Services or of any components or portions of Oracle PaaS and IaaS Cloud Services other than the components specified in the Oracle Cloud Security Testing Policy.

In addition to other rights that Oracle has in this Agreement and Your order, Oracle has the right

to take remedial action if the Acceptable Use Policy is violated, and such remedial action may include removing or disabling access to material that violates the policy. With respect to the preceding sentence, Oracle shall make reasonable efforts to provide you with advance notice, when practical, in Oracle's reasonable discretion based on the nature of the circumstances.

2. OWNERSHIP RIGHTS AND RESTRICTIONS

2.1 You or Your licensors retain all ownership and intellectual property rights in and to Your Content. Oracle or its licensors retain all ownership and intellectual property rights in and to the Services, derivative works thereof, and anything developed or delivered by or on behalf of us under this Agreement.

2.2 You may have access to Third Party Content through use of the Services. Unless otherwise stated in Your order, all ownership and intellectual property rights in and to Third Party Content and the use of such content is governed by separate third party terms between You and the third party.

2.3 You grant us the right to host, use, process, display and transmit Your Content to provide the Services pursuant to and in accordance with this Agreement and Your order. You have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of Your Content, and for obtaining all rights related to Your Content required by Oracle to perform the Services.

2.4 You may not, and may not cause or permit others to: (a) modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, republish or copy any part of the Services (including data structures or similar materials produced by programs); (b) access or use the Services to build or support, directly or indirectly, products or services competitive to Oracle; or (c) license, sell, transfer, assign, distribute, outsource, permit timesharing or service bureau use of, commercially exploit, or make available the Services to any third party except as permitted by this Agreement or Your order.

3. NONDISCLOSURE

3.1 By virtue of this Agreement, the parties may disclose information that is confidential ("Confidential Information"). To the extent permitted by law, Confidential Information shall be limited to Your Content residing in the Services, and all information clearly identified as confidential at the time of disclosure.

3.2 A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party.

3.3 Subject to applicable law, each party agrees not to disclose the other party's Confidential Information to any third party other than as set forth in the following sentence for a period of five years from the date of the disclosing party's disclosure of the Confidential Information to the receiving party; however, Oracle will protect the confidentiality of Your Content residing in the Services for as long as such information resides in the Services, except for Personal Information, which shall be held in confidence in perpetuity. Each party may disclose Confidential Information only to those employees, agents or subcontractors who are required to protect it against unauthorized disclosure in a manner no less protective than required under this

Agreement, and each party may disclose the other party's Confidential Information in any legal proceeding or to a governmental entity as required by law. Oracle will protect the confidentiality of Your Content residing in the Services in accordance with the Oracle security practices defined as part of the Service Specifications applicable to Your order.

The parties acknowledge and agree that You and this Agreement are subject to applicable freedom of information or open records law. Should you receive a request under such law for Oracle's Confidential Information, You agree to give Oracle adequate prior notice of the request and before releasing Oracle's Confidential Information to a third party, in order to allow Oracle sufficient time to seek injunctive relief or other relief against such disclosure.

3.4 Notwithstanding the foregoing, following the end of the Service Period for Cloud Services acquired by a User, Oracle will continue to protect the User's Content from such Services which remain in Oracle's possession (including during any applicable retrieval period as specified in the Oracle Hosting & Delivery Policies) pursuant to the terms of this agreement, until such Content is either returned to the User or deleted from the Oracle Cloud Services environments.

4. PROTECTION OF YOUR CONTENT

4.1 In performing the Services, Oracle will comply with the Oracle privacy policy applicable to the Services ordered. Oracle privacy policies are available at http://www.oracle.com/us/legal/privacy/overview/index.html .

4.2 Oracle's *Data Processing Agreement for Oracle Cloud Services* (the "Data Processing Agreement"), which is available at http://www.oracle.com/dataprocessingagreement and incorporated herein by reference, describes how Oracle will process Personal Data that You provide to us as part of Oracle's provision of the Services, unless stated otherwise in Your order. You agree to provide any notices and obtain any consents related to Your use of, and Oracle's provision of, the Services.

4.3 Oracle will protect Your Content as described in the Service Specifications, which define the administrative, physical, technical and other safeguards applied to Your Content residing in the Services and describe other aspects of system management applicable to the Services. Oracle and its affiliates may perform certain aspects of the Services (e.g., administration, maintenance, support, disaster recovery, data processing, etc.) from locations and/or through use of subcontractors, worldwide.

4.4 You are responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from Your Content, including any viruses, Trojan horses, worms or other harmful programming routines contained in Your Content, or from Your use of the Services in a manner that is inconsistent with the terms of this Agreement. You may disclose or transfer, or instruct us to disclose or transfer in writing, Your Content to a third party, and upon such disclosure or transfer Oracle is no longer responsible for the security or confidentiality of such content and applications outside of Oracle.

4.5 Unless otherwise specified in the Service Specifications, Oracle's Services can only accept, and you will only provide, personal data which does not have data protection, security controls or regulatory requirements (e.g., Oracle Payment Card Industry (PCI)) in addition to those applicable to personally identifiable information. If available, a User may purchase Services (e.g., Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services, etc.) designed to address particular data protection requirements. The applicable Service Specifications will identify whether the Services are designed to address data protection requirements applicable to PCI and/or Protected Health Information (PHI) and/or other

types of protected data. Additionally, upon a User's written request, the CSP will identify if the Services a User is requesting to purchase are designed to address data protection requirements applicable to PCI and/ or PHI and/or other types of protected data.

5. WARRANTIES, DISCLAIMERS AND EXCLUSIVE REMEDIES

5.1 Each party represents that it has validly entered into this Agreement and that it has the power and authority to do so. Oracle warrants that during the Services Period, Oracle will perform the Services using commercially reasonable care and skill in all material respects as described in the Service Specifications. If the Services provided to You were not performed as warranted, You must promptly provide us with a written notice that describes the deficiency in the Services (including, as applicable, the service request number notifying us of the deficiency in the Services).

5.2 ORACLE DOES NOT WARRANT THAT THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, THAT ORACLE WILL CORRECT ALL SERVICES ERRORS, OR THAT THE SERVICES WILL MEET YOUR REQUIREMENTS OR EXPECTATIONS. ORACLE IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM YOUR CONTENT OR THIRD PARTY CONTENT OR SERVICES PROVIDED BY THIRD PARTIES.

5.3 FOR ANY BREACH OF THE SERVICES WARRANTY, YOUR EXCLUSIVE REMEDY AND ORACLE'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, YOU MAY END THE DEFICIENT SERVICES AND ORACLE WILL REFUND TO MYTHICS, INC., AND MYTHICS, INC. WILL IN TURN REFUND TO YOU THE FEES PAID FOR THE DEFICIENT SERVICES FOR THE PERIOD OF TIME DURING WHICH THE SERVICES WERE DEFICIENT.

5.4 TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. LIMITATION OF LIABILITY

6.1 IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES NOR ORACLE BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, OR ANY LOSS OF REVENUE OR PROFITS, DATA, OR DATA USE, SALES, GOODWILL, OR REPUTATION.

6.2 IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ORACLE AND ORACLE'S AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR YOUR ORDER, WHETHER IN CONTRACT TORT OR OTHERWISE, EXCEED THE TOTAL AMOUNTS ACTUALLY PAID TO ORACLE FOR THE SERVICES UNDER THE ORDER GIVING RISE TO THE LIABILITY IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY LESS ANY REFUNDS OR CREDITS RECEIVED UNDER SUCH ORDER.

7. INDEMNIFICATION

7.1 Subject to the terms of this Section 7 (Indemnification), if a third party makes a claim against either You or Oracle ("Recipient" which may refer to You or Oracle depending upon which party received the Material), that any information, design, specification, instruction, software, service, data, hardware, or material (collectively, "Material") furnished by either You or Oracle ("Provider" which may refer to You or Oracle depending on which party provided the Material) and used by the Recipient infringes the third party's intellectual property rights, the Provider, at the Provider's sole cost and expense, will to the extent not prohibited by law, defend the Recipient against the claim and indemnify the Recipient from the damages, liabilities, costs and expenses awarded by

the court to the third party claiming infringement or the settlement agreed to by the Provider, if the Recipient does the following:

a. notifies the Provider promptly in writing, not later than 30 days after the Recipient receives notice of the claim (or sooner if required by applicable law);
b. gives the Provider sole control of the defense and any settlement negotiations, to the extent not prohibited by law; and
c. gives the Provider the information, authority and assistance the Provider needs to defend against or settle the claim.

7.2 If the Provider believes or it is determined that any of the Material may have violated a third party's intellectual property rights, the Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Oracle's ability to meet its obligations under the relevant order, then Oracle may, upon 30 days prior written notice, terminate the order. If such Material is third party technology and the terms of the third party license do not allow Oracle to terminate the license, then Oracle may, upon 30 days prior written notice, end the Services associated with such Material and refund to Mythics, Inc., and Mythics, Inc. will in turn refund to You any unused, prepaid fees for such Services.

7.3 The Provider will not indemnify the Recipient if the Recipient (a) alters the Material or uses it outside the scope of use identified in the Provider's user or program documentation or Service Specifications, or (b) uses a version of the Material which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was made available to the Recipient. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon any Material not furnished by the Provider. Oracle will not indemnify You to the extent that an infringement claim is based on Third Party Content or any Material from a third party portal or other external source that is accessible or made available to You within or by the Services (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, marketing data from third party data providers, etc.).

7.4 This Section 7 provides the parties' exclusive remedy for any infringement claims or damages.

8. TERM AND TERMINATION

8.1 RESERVED

8.2 Oracle may suspend Your or Your Users' access to, or use of, the Services if Oracle believes

that (a) there is a significant threat to the functionality, security, integrity, or availability of the Services or any content, data, or applications in the Services; (b) You or Your Users are accessing or using the Services to commit an illegal act; or (c) there is a violation of the Acceptable Use Policy. When reasonably practicable and lawfully permitted, Oracle will provide You with advance notice of any such suspension. Oracle will use reasonable efforts to re- establish the Services promptly after Oracle determines that the issue causing the suspension has been resolved. During any suspension period, Oracle will make Your Content (as it existed on the suspension date) available to You. Any suspension under this paragraph shall not excuse You from Your obligation to make payments under this Agreement.

8.3 RESERVED

8.4 Termination of the Agreement will not affect orders that are outstanding at the time of termination. Those orders will be performed according to their terms as if this Agreement were still in full force and effect. However, those orders may not be renewed or extended subsequent to termination of this Agreement.

8.5 For a period of no less than 60 days after the end of the Services Period of an order, Oracle will make Your Content (as it existed at the end of the Services Period) available for retrieval by You. At the end of such 60 day period, and except as may be required by law, Oracle will delete or otherwise render inaccessible any of Your Content that remains in the Services.

8.6 Provisions that survive termination or expiration of this Agreement are those relating to limitation of liability, indemnification, payment and others which by their nature are intended to survive.

9. THIRD-PARTY CONTENT, SERVICES AND WEB SITES

9.1 The Services may enable You to link to, transmit Your Content to, or otherwise access third parties' websites, platforms, content, products, services, and information. Oracle does not control and are not responsible for such third parties' websites, platforms, content, products, services, and information.

9.2 Any Third Party Content Oracle makes accessible is provided on an "as-is" and "as available" basis without any warranty of any kind. You acknowledge and agree that Oracle is not responsible for, and have no obligation to control, monitor, or correct, Third Party Content. Oracle disclaims all liabilities arising from or related to Third Party Content.

9.3 You acknowledge that: (i) the nature, type, quality and availability of Third Party Content may change at any time during the Services Period, and (ii) features of the Services that interoperate with third parties such as Facebook™, YouTube™ and Twitter™, etc. (each, a "Third Party Service"), depend on the continuing availability of such third parties' respective application programming interfaces (APIs). Oracle may need to update, change or modify the Services under this Agreement as a result of a change in, or unavailability of, such Third Party Content, Third Party Services or APIs. If any third party ceases to make its Third Party Content or APIs available on reasonable terms for the Services, as determined by Oracle in its sole discretion, Oracle may cease providing access to the affected Third Party Content or Third Party Services without any liability to You. Any changes to Third Party Content, Third Party Services or APIs, including their unavailability, during the Services Period does not affect Your obligations under this Agreement or the applicable order, and You will not be entitled to any refund, credit or other compensation due to any such changes.

10. SERVICE MONITORING, ANALYSES AND ORACLE SOFTWARE

10.1 Oracle continuously monitors the Services to facilitate Oracle's operation of the Services; to help resolve Your service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. Oracle monitoring tools do not collect or store any of Your Content residing in the Services, except as needed for such purposes. Oracle does not monitor, and does not address issues with, non-Oracle software provided by You or any of Your Users that is stored in, or run on or through, the Services. Information collected by Oracle monitoring tools (excluding Your Content) may also be used to assist in managing Oracle's product and service portfolio, to help Oracle address deficiencies in its product and service offerings, and for license management purposes.

10.2 Oracle may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). Oracle may make Service Analyses publicly available; however, Service Analyses will not incorporate Your Content or Confidential Information in a form that could serve to identify You or any individual, and Service Analyses do not constitute Personal Data. Oracle retains all intellectual property rights in Service Analyses.

10.3 Oracle may provide You with online access to download certain Oracle Software for use with the Services. If Oracle licenses Oracle Software to You and do not specify separate terms for such software, then such Oracle Software is provided as part of the Services and You have the non-exclusive, worldwide, limited right to use such Oracle Software, subject to the terms of this Agreement and Your order, solely to facilitate Your use of the Services. You may allow Your Users to use the Oracle Software for this purpose, and You are responsible for their compliance with the license terms. Your right to use Oracle Software will terminate upon the earlier of Oracle's notice (by web posting or otherwise) or the end of the Services associated with the Oracle Software. If Oracle Software is licensed to You under separate third party terms, then Your use of such software is governed by the separate third party terms.

11. EXPORT

11.1 Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Services. Such export laws govern use of the Services (including technical data) and any Services deliverables provided under this Agreement, and You and Oracle each agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). You agree that no data, information, software programs and/or materials resulting from Services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

11.2 You acknowledge that the Services are designed with capabilities for You and Your Users to access the Services without regard to geographic location and to transfer or otherwise move Your Content between the Services and other locations such as User workstations. You are solely responsible for the authorization and management of User accounts across geographic locations, as well as export control and geographic transfer of Your Content.

12. FORCE MAJEURE

RESERVED

13. NOTICE

13.1 Any notice required under this Agreement shall be provided to the other party, and Oracle, in writing. If You have a legal dispute with Oracle or if You wish to provide a notice under the Indemnification Section of this Agreement, or if You become subject to insolvency or other similar legal proceedings, You will promptly send written notice to: Oracle America, Inc., 500 Oracle Parkway Redwood Shores, CA 94065, Attention: General Counsel, Legal Department.

13.2 Oracle may give notices applicable to Oracle's Cloud Services customer base by means of a general
notice on the Oracle portal for the Cloud Services, and notices specific to You by electronic mail to Your e-mail address on record in Oracle's account information or by written communication sent by first class mail or pre- paid post to Your address on record in Oracle's account information.

14. ASSIGNMENT

You may not assign this Agreement or give or transfer the Services, or any interest in the Services, to another individual or entity.

15. OTHER

15.1 Oracle is an independent contractor and we agree that no partnership, joint venture, or agency relationship exists between Oracle, Mythics, Inc., and You. We are each responsible for paying our own employees, including employment related taxes and insurance. You understand that Oracle's business partners and other third parties, including any third parties with which Oracle has an integration agreement or that are retained by You to provide consulting or implementation services or applications that interact with the Cloud Services, are independent of Oracle and are not Oracle's agents. Oracle is not liable for, bound by, or responsible for any problems with the Services, Your Content or Your Applications arising due to any acts of any such business partner or third party, unless the business partner or third party is providing Services as an Oracle subcontractor on an engagement ordered under this Agreement and, if so, then only to the same extent as Oracle would be responsible for Oracle resources under this Agreement. This Agreement is entered exclusively between You and Mythics, Inc. While Oracle has no contractual relationship with You, Oracle is a third party beneficiary of this Agreement.

15.2 If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective and such term shall be replaced with another term consistent with the purpose and intent of this Agreement.

15.3 Except for actions for nonpayment or breach of Oracle's proprietary rights, no action, regardless of form, arising out of or relating to this Agreement may be brought by either party more than four years after the cause of action has accrued.

15.4 Prior to entering into an order governed by this Agreement, You are solely responsible for determining whether the Services meet Your specific technical, business or regulatory requirements. Oracle will cooperate with Your efforts to determine whether use of the standard Services are consistent with those requirements. Additional fees may apply to any additional work performed by Oracle or changes to the Services. You remain solely responsible for Your

regulatory compliance in connection with Your use of the Services.

15.5 Upon forty-five (45) days written notice and no more than once every twelve (12) months, Oracle may audit Your compliance with the terms of this Agreement and Your order. You agree to cooperate with Oracle's audit and to provide reasonable assistance and access to information. Any such audit shall not unreasonably interfere with Your normal business operations. Any such audit shall be limited to information reasonably necessary to allow the Contractor or the CSP to determine whether a User's use of a Service is in compliance with this agreement and the applicable order.

16. ENTIRE AGREEMENT

16.1 RESERVED

16.2 Oracle may update the Service Specifications, including by posting updated documents on Oracle's websites, without the need for an amendment signed by authorized representatives of the parties. Except as set forth in Section 15.1, no third party beneficiary relationships are created by this Agreement.

17. AGREEMENT DEFINITIONS

17.1. "**Oracle Software**" means any software agent, application or tool that Oracle makes available to You for download specifically for purposes of facilitating Your access to, operation of, and/or use with, the Services.

17.2. "**Program Documentation**" refers to the user manuals, help windows, readme files for the Services and any Oracle Software. You may access the documentation online at http://oracle.com/contracts or such other address specified by Oracle.

17.3. "**Service Specifications**" means the following documents, as applicable to the Services under Your order: (a) the Cloud Hosting and Delivery Policies, the Program Documentation, the Oracle service descriptions, and the Data Processing Agreement, available at www.oracle.com/contracts; (b) Oracle's privacy policy, available at http://www.oracle.com/us/legal/privacy/overview/index.htm; and (c) any other Oracle documents that are referenced in or incorporated into Your order. The following do not apply to any non-Cloud Oracle service offerings acquired in Your order, such as professional services: the Cloud Hosting and Delivery Policies, Program Documentation, and the Data Processing Agreement. The following do not apply to any Oracle Software that is provided by Oracle as part of the Services and governed by the terms of this Agreement: the Cloud Hosting and Delivery Policies, Oracle service descriptions, and the Data Processing Agreement.

17.4. "**Third Party Content**" means all software, data, text, images, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of Oracle that You may access through, within, or in conjunction with Your use of, the Services. Examples of Third Party Content include data feeds from social network services, rss feeds from blog posts, Oracle data marketplaces and libraries, dictionaries, and marketing data. Third Party Content' does not include content that is provided by Oracle, including Oracle Software (which may include software either owned by Oracle or licensed by Oracle) or embedded functionality. Content that Oracle owns or licenses from others and provides as part of the Services is deemed to be 'provided by Oracle.

17.5. "**Users**" means those employees, contractors, and end users, as applicable, authorized by You or on Your behalf to use the Services in accordance with this Agreement and Your order. For Services that are specifically designed to allow Your clients, agents, customers, suppliers or other third parties to access the Cloud Services to interact with You, such third parties will be considered "Users" subject to the terms of this Agreement and Your order.

17.6. "**Your Content**" means all software, data (including Personal Data as that term is defined in the Data Processing Agreement for Oracle Cloud Services described in this Agreement), text, images, audio, video, photographs, non-Oracle or third party applications, and other content and material, in any format, provided by You or any of Your Users that is stored in, or run on or through, the Services. Services under this Agreement, Oracle Software, other Oracle products and services, and Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the term "Your Content"

18. CLOUD SERVICES EFFECTIVE DATE

The Effective Date of this Cloud Services Agreement is _____ (DATE TO BE COMPLETED BY MYTHICS, INC.).

EXHIBIT G
Data Processing Agreement for Oracle Services

("Data Processing Agreement")

Version June 26, 2019

1. Scope and Applicability

1.1 This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

1.2 Reserved.

2. Responsibility for Processing of Personal Information and Your instructions

2.1 You are a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Oracle will Process Personal Information solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

2.4 Oracle will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

2.5 Unless otherwise specified in the Services Agreement, You may not provide Oracle with any sensitive or special Personal Information that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Data Processing Agreement or Services Agreement.

3. Privacy Inquiries and Requests from Individuals

3.1 If You receive a request or inquiry from an Individual related to Personal Information processed by

Oracle for the provision of Services, You can either (i) securely access Your Services environment that holds Personal Information to address the request, or (ii) to the extent such access is not available to You, submit a "service request" via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to Oracle on how to assist You with such request.

3.2 If Oracle directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

4. Oracle Affiliates and Third Party Subprocessors

4.1 To the extent Oracle engages Third Party Subprocessors and/or Oracle Affiliates to Process Personal Information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement. Oracle is responsible for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

5. Reserved

6. Security and Confidentiality

6.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services:

- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: http://www.netsuite.com/portal/resource/terms-of-service.shtml;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: https://www.oracle.com/support/policies.html;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: http://www.oracle.com/us/corporate/contracts/consulting-services/index.html.

6.2 All Oracle and Oracle Affiliates employees, as well as any Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

7. Audit Rights

7.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

7.2 If a third party is to conduct the audit, the third party must be mutually agreed to by You and Oracle (except if such third party is a Regulator). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory or legal confidentiality obligation.

7.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan.

7.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

7.5 Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

7.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

7.7 Without prejudice to the rights granted in Section 7.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

8. Incident Management and Breach Notification

8.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence.

8.2 Oracle will notify you of a confirmed Personal Information Breach without undue delay but at the latest within 24 hours. As information regarding the Personal Information Breach is collected or

otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Personal Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of Personal Information that were the subject of the Personal Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Personal Information Breach.

9. Return and Deletion of Personal Information

9.1 Upon termination of the Services, Oracle will promptly return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Information on Oracle systems or Services environments, except as otherwise stated in the Services Agreement.

9.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by Oracle as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

10. Legal Requirements

10.1 Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

10.2 Oracle will promptly inform You of requests to provide access to Personal Information, unless otherwise required by law.

11. Definitions

"**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, which may include Applicable European Data Protection Law.

"**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended; and (iii) the UK Data Protection Act 2018.

"**Europe**" means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway; (ii) Switzerland and (iii) the UK after it withdraws from the EU.

"**Individual**" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

"**Process/Processing**", "**Controller**", "**Processor**" and "**Binding Corporate Rules**" (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

"**Oracle Affiliate(s)**" means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in Section 4.

"**Oracle Intra-Company Data Transfer and Mandate Agreement"** means the Oracle Intra-Company

Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

"**Oracle Processor Code**" means Oracle's Privacy Code for Processing Personal Information of Customer Individuals referenced in the European DPA Addendum.

"**Oracle**" means the Oracle Affiliate that has executed the Services Agreement.

"**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.

"**Personal Information Breach"** means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Information.

"**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.

"**Services**" or the equivalent terms "Service Offerings" or "services" means the Cloud, Advanced

Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

"**Services Agreement**" means (i) the applicable order for the Services you have purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications.

"**Third Party Subprocessor**" means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in Section 4.

"**You**" means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.

Data Processing Agreement for Oracle Services v 06262019