STATE OF CALIFORNA DEPARTMENT OF TECHOLOGY
CONTRACT ID: CON0000202
MICROSOFT ONLINE SERVICES

ATTEST:
STEPHANIE R. DIETZ, CITY CLERK

BY:_____
Assistant/Deputy City Clerk

APPROVED AS TO FORM:

BY: _____ 5/14/21
City Attorney Date

ACCOUNT DATA:

BY:_____
Verified by Finance Officer

CONTRACT

CA DEPT OF TECHNOLOGY

CALIFORNIA DEPT OF TECHNOLOGY
ADMIN WAREHOUSE
10173 CROYDON WAY STE 4
SACRAMENTO CA 95827
USA

Supplier 0000003507
CRAYON SOFTWARE EXPERTS, LLC
GREG LANDRY
12221 MERIT DR - STE 800
DALLAS TX 75251
USA

Dispatch via Print

Contract ID			Page
CON0000202			1 of 28
Contract Dates	**Currency**	**Rate Type**	**Rate Date**
03/01/2021 to 02/28/2026	USD	CRRNT	PO Date
Description:		**Contract Maximum**	
Microsoft Online Services		257,189,482.04	
Allow Open Item Reference			

Tax Exempt? Y Tax Exempt ID: 0

Exhibit A: Statement of Work	pages 2-7
Exhibit A-1: M365 GCC E5 Licensing Structure	page 8
Exhibit B: Payment and Invoicing	page 9
Exhibit C: Cost Worksheet Details	pages 10-11
*Exhibit C – 1: Cost Worksheet	
*Exhibit C – 2: Supplemental Cost Worksheet	
Exhibit D: Special Terms and Conditions to Safeguard Federal Tax Information	pages 12-20
Exhibit E: Security and Data Protection	page 21
Exhibit F: HIPAA Business Associate Agreement	page 22-27
*Exhibit G: State of California Terms and Conditions	page 28

*Items with the Asterisk (*) are hereby incorporated by reference as if attached hereto.

Please note that payment on invoices presented for the items in this Contract are not effective until subsequent Purchase Orders per tenant enrollment are issued and State Budget appropriation is approved annually to sufficiently fund the invoices. If the funds to effect payment are not authorized, Contractor understands the State may cancel this order and the Contractor agrees to take back any software and/or terminate subscriptions furnished under this contract, terminate any services supplied to the State under this contract, and relieve the State of any obligation therefore.

Final = The price is final after adjustments
Hard = Apply adjustments regardless of other adjustments
Skip = Skip adjustments if any other adjustments have been applied

Authorized Signature

Jennifer Herrera

Feb 28, 2021

EXHIBIT A: STATEMENT OF WORK

1. Contract Description:

a. **Crayon Software Experts LLC** (hereinafter referred to as the "Contractor") agrees to provide the California Department of Technology and its customers, (hereinafter referred to as the "State," or the "Licensee") Microsoft Online Services Subscriptions as identified in Exhibit C of this Agreement. As part of a statewide Enterprise Agreement (EA), Contractor must:

- Provide option(s) for departments to standardize on Microsoft Security, Compliance and Communications
- Create a new enrollment with Microsoft Security, Compliance and Communications on a five (5) year term
- Ensure applicable credits are applied to Year 1 and Year 2 (If applicable) cost based on customer's existing agreements prior to invoicing CDT
- Awarded Contractor may not mark up or mark down the credited amount to be applied to the Enrollment. The credit amount(s) will be verified prior to award.
- Following award, but prior to PO execution, Contractor shall complete a post award Supplemental Cost Worksheet with net pricing reflective of applicable discounts and credits.
- Provide a negotiated discount applied from Software Assurance (SA) base across term of the new agreement
- Provide discounts based on committed users and applied over the term of the agreement with applicable tiered discount structure at anniversary. For products not already identified on RFO, Contractor's quoted pricing will not exceed the highest margin item on RFO.

b. Government Community Cloud availability and roadmap

1) At the outset, CA Affiliates will have access to the three main components of M365 E5 including:

- Office 365 E5 – advanced collaboration, voice and data analytics
- Enterprise Mobility and Security E5 – includes Defender for Identity and Microsoft Cloud Application Security
- Windows E5 – includes Defender for Endpoint (formerly Windows Defender Advanced Threat Protection)

2) Government Community Cloud (GCC) Roadmap

- Defender for Endpoint will be available at the inception of the agreement
- Defender for Identity (AATP) and Microsoft Cloud Application Security will initially be commercial instances but will become available in the GCC in the second quarter of the calendar year
- These new conformant offerings will fold together into a new unified "Microsoft 365 Defender" portal to view the M365 security posture in a combined view (Defender for Office 365 {O365 ATP}, Defender for Endpoint, Defender for Identity, Cloud App Security)

c. The Microsoft Online Services Subscriptions will be provided by the manufacturer, Microsoft, under the Department of Technology Procurement Contract (**CON** 20-0000202) and subsidiary Purchase Orders issued off of the Contract.

d. The Request for Offer (RFO) and Contractor response to RFO # 20-0038064 are hereby incorporated by reference and made a part of this Agreement as if attached hereto.

e. Under the terms of this agreement, each State customer will be their own tenant.

f. Terms and Conditions of Department of General Services (DGS) Software Licensing Program (SLP), which was recently amended from Software Cooperative Agreement (SCA), County of Riverside RFQ no. RIVCO-2020-RFQ-0000048 and Microsoft Master Agreement no. 8084445 shall apply to this Contract though the life of its term.

g. Upon execution, the Contractor will be provided a Procurement Contract for the Contract total and term. Purchase Orders (PO) will subsequently be issued to Contractor for each tenant. Contractor to invoice CDT separately for each customer tenant.

2. Term:

The term of the Agreement shall be for **five (5) years** (60 full calendar months) from receipt and acceptance of subscription product and support. Estimated Agreement start date is **3/01/2021** with an estimated expiration date of **2/28/2026, or 60 full calendar months after the Effective Date, whichever comes later**. These dates are only estimates and may be changed by an amendment to the Agreement (CDT Procurement Contract or Purchase Order issued).

The Effective Date of this enrollment will be the date it is accepted and processed by Microsoft and available for use in Customer Affiliate portals. The anniversary date schedule shall be as follows:

- 1st anniversary 12 full calendar months from the effective date.
- 2nd anniversary 24 full calendar months from the effective date.
- 3rd anniversary 36 full calendar months from the effective date.
- 4rth anniversary 48 full calendar months from the effective date.
- Expiration will occur 60 full calendar months from the effective date.

Any Procurement Contract or Purchase Orders issued for services that begin or extend beyond the term of the Riverside County Contract shall be subject to the terms of the Riverside County Contract.

3. California Department of Technology Responsibilities:

a. Designate a person (Program Manager) to whom all Contractor communication may be addressed and who has the authority to act on all aspects of the service. This person may review the Agreement and associated documents with the Contractor to ensure understanding of the responsibilities of both parties.

b. Provide timely review and approval of information and documentation provided by the Contractor to perform its obligations.

4. Licensee Site/Location:

The "Licensee Site" shall mean the **California Department of Technology and its customers tenants** as identified in this Agreement, which Licensee represents, is operated or controlled by Licensee. Licensee may change the Licensee Site to another location located within the United States without incurring additional charges.

5. License Type:

Annual Software as a Service Subscription - Right-To-Use License. The State Cloud Computing-Software as a Service (SaaS) (Effective 6/7/2019) and IT General Provisions (GSPD 09/05/14) will take precedence over the software hard copy or "click to accept" terms and conditions.

6. Installed on:

All software and hardware installed will be located at the manufacturer's site.

7. True-ups:

The State may deploy additional products and support services beyond the products and/ or support identified in the initial Microsoft Enrollments.

a. Additional quantities of the Microsoft products/services procured in the initial Agreement may be added or decremented subject to the Subscription License Reductions section of the Enterprise Enrollment by the State during the term of this Agreement. Products are price protected (fixed prices throughout the enrollment period) and shall be priced by the Contractor at the original price identified for the Enterprise License Agreement products listed in Exhibit C – Cost Worksheet.

b. The Contractor shall notify the State of any change in the product/service catalog that could increase the cost of services being provided to the State

c. The Contractor shall provide the State with an annual report of licenses added and decremented during the true-up period.

d. True-ups to add or decrement license counts will only occur once a year (prior to anniversary date).

   1) Contractor to provide customer affiliates with budgetary quote for annual reconciliation sixty (60) days prior to anniversary dates.

   2) True-downs or decrements must be fully processed by the Contractor prior to PO anniversary date.

8. Contractor Responsibilities:

Contractor to provide dedicated staff/dedicated teams – with clearly identified, roles and responsibilities, path of escalation, list primary and back up.

a. The Contractor shall designate a primary and secondary contact person to whom all Contract/PO communications may be addressed and who has the authority to act on all aspects of the services.

b. The Contractor shall provide a path of escalation for all communication and Contract/PO related matters.

c. The Contractor shall ensure dedicated staff are available during state business hours of 7:30 AM, PT to 5:30 PM, PT.

d. Contract must adhere to invoicing requirements listed in Exhibit B.

e. Contractor shall provide CDT with confirmation upon receipt of PO or PO amendment.

f. Contractor shall provide CDT with Booking Confirmation verifying order has been submitted to Microsoft.

g. All EA Enrollment documents requiring electronic signature shall be sent to a designated CDT contact and not Customer Affiliate.

h. Following execution of consolidated EA, Contractor will schedule a kick off meeting within 5-10 business days with CDT to discuss CDT billing and invoicing requirements and develop a plan for collaboration and streamlining of billing and invoicing procedures.

i. Contractor and Microsoft shall not offer or discuss any new product or non-GCC Add-Ons with Customer Affiliates without approval from CDT Contract Administrator.

9. 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 set below 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 and directed to the following addresses below:

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

State Agency		Manufacturer	
California Department of Technology		Microsoft	
Attn:	CDT IT Program Management	Attn:	Marsha Brown
		Phone:	213-806-7493
E-mail:	ITPM@state.ca.gov	E-mail :	marshab@microsoft.com

Contract inquiries should be addressed to:

State Agency		Contractor	
California Department of Technology, Acquisitions & IT Program Management Branch		Crayon Software Experts LLC	
Attn:	CDT IT Program Management	Attn:	Greg Landry
Address:	PO Box 1810 Rancho Cordova, CA. 95741	Address:	12221 Merrit Drive, STE 800 Dallas, TX 75251
		Phone:	469-329-0263
E-mail:	ITPM@state.ca.gov	E-mail:	greg.landry@crayon.com

10. Maintenance/ Technical Support:

The Contractor shall ensure that maintenance and support are provided by Microsoft throughout the term of the Agreement.

Web Support:

https://www.microsoft.com/licensing/servicecenter/default.aspx

11. Advertising of Data:

The Contractor and any service providers are not authorized to use, sell, resell, package or repackage or publicly display any information or data without the express written approval of the State. This restriction includes key-word searching or data mining of state data. Advertising is not allowed in any of these services or to any of the contacts associated with these services.

12. Amendments:

Consistent with the terms and conditions of the original RFO, and upon mutual consent, the Department of Technology 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, as required. No verbal understanding or agreement not incorporated into the Agreement is binding on any of the parties.

13. 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's Primary Contact will determine the next level of severity, and notify the appropriate State and Manufacturer 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: CDT Contract Administrator
Second Level: CDT Branch Chief
Third Level: CDT Deputy Director

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

First Level: Contractor Support Specialist
Second Level: Contractor Support Manager
Third Level: Contractor Duty Manager

d. The Manufacturer personnel include, but are not limited to the following:

First Level: Contractor Support Specialist
Second Level: Contractor Support Manager
Third Level: Contractor Duty Manager

14. Termination Provisions:

The State may exercise its option to terminate this Agreement at any time with thirty (30) calendar days' prior written notice.

15. Change of Channel Partner

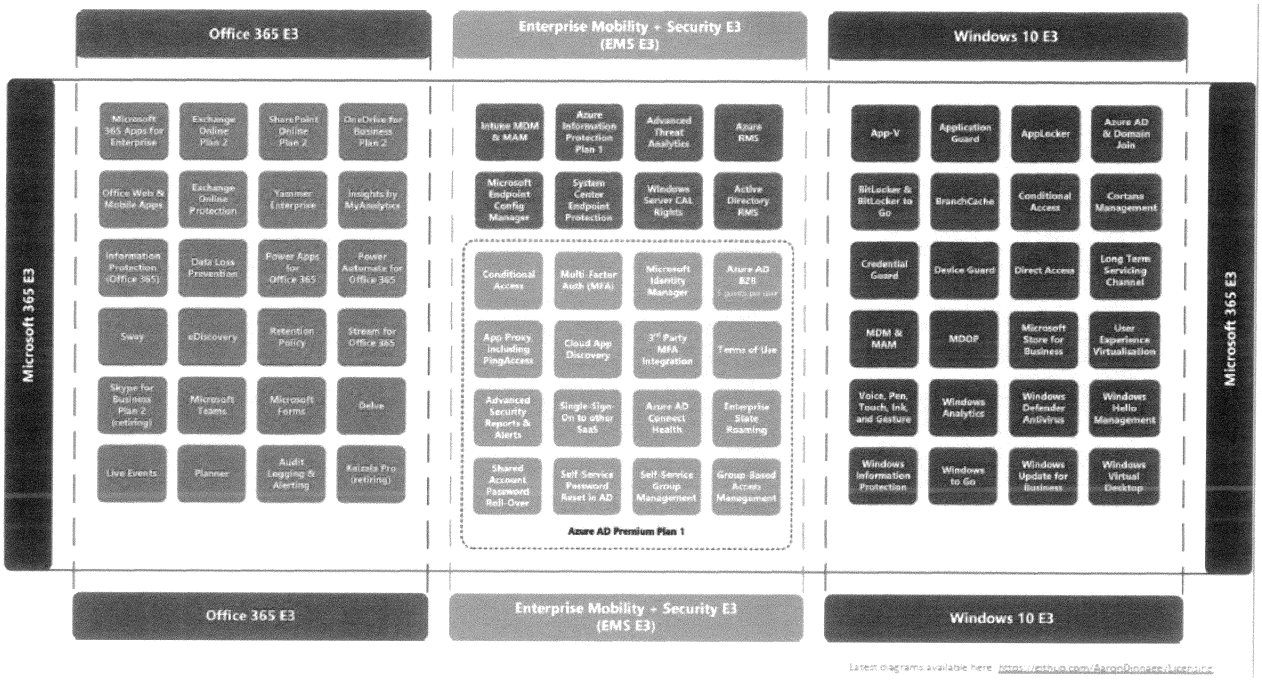
If Contractor fails to meet the Contract, CDT and or Customer Affiliate requirements CDT may exercise right to change channel partner.

16. Adding New State of California Affiliates to this Consolidated Enrollment:

For a period of one (1) year after the Effective Date, Microsoft shall accommodate existing State of California Affiliate Enrollments when that Enrolled Affiliate requests to enter the consolidated enrollment and terminate their existing Enrollments. Affiliates include but are not limited to State, City, County and local affiliates. Following this period, additional State of California Affiliate Enrollments may join the consolidation at either the anniversary or expiration of their current Enrollments.

EXHIBIT A-1: M365 GCC E5 LICENSING STRUCTURE

https://www.microsoft.com/en-us/microsoft-365/enterprise/e5



Latest diagrams available here: https://github.com/AaronDinnage/Licensing

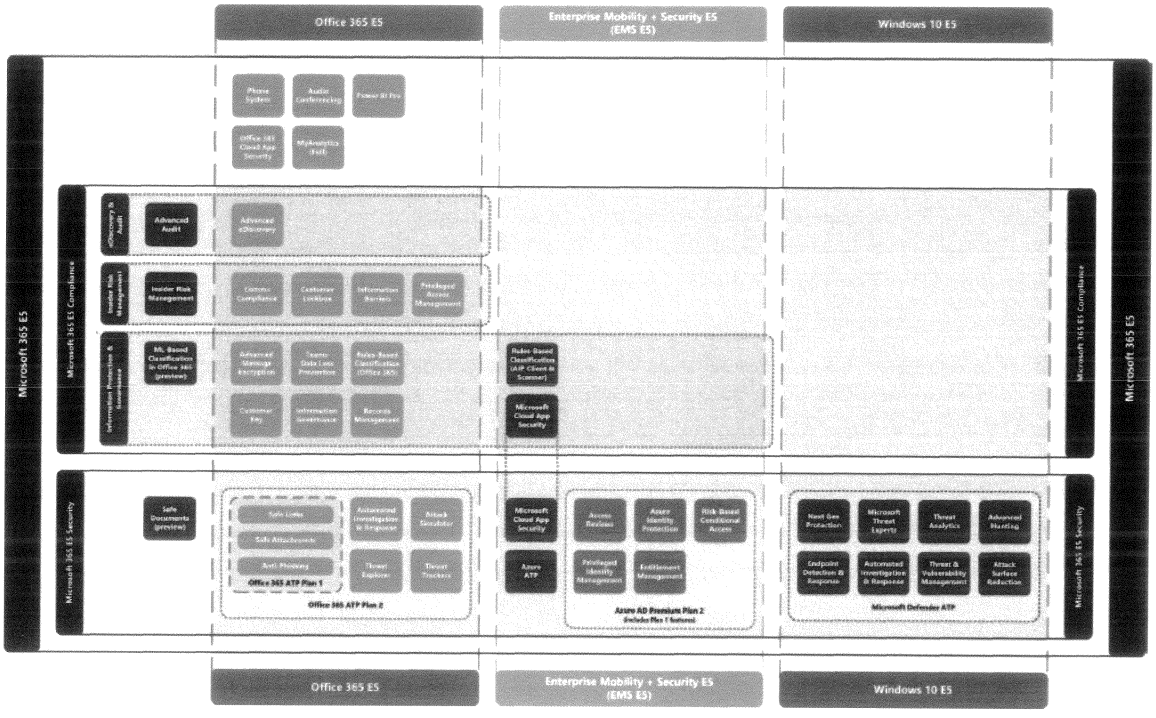


EXHIBIT B: PAYMENT AND INVOICING

1. Payment/Invoicing:

a. Payment will be made in advance for the subscription year and upon receipt of a **correct** invoice. Invoice may be submitted on or after the first day of the term referenced on the RFO and executed PO. **The invoice shall include booking confirmation of the Department of Technology order per each environment; including but not limited to, the Contract number, the individual Customer PO number, the Customer Department, the EA/Tenant ID/number, the product name, SKU number, unit cost, extended cost, code (if applicable), must reference a specific PO line item, term dates and include PO amendment number if applicable**; and shall reference the Agency Order Number and the Microsoft Enterprise License Agreement (MELA) Software Licensing Program (SLP) number **SCA-19-70-0204C** in **TRIPLICATE** to:

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

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

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

OR

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

c. Contractor shall work with CDT to create a template for invoice that meets CDT requirements.

d. If there is a change in cost to a license or if the start date for licenses is changed so that it impacts pricing i.e., term and activation of licenses falls after the 2nd of the month, and so billing begins following month, Contractor must provide product pricing change update and quote to the Customer entity so that an amendment can be executed to the Customer's PO to reflect the correct pricing.

e. Ensure applicable credits are applied to Year 1 and Year 2 (If applicable) cost based on customer's existing agreements prior to invoicing CDT

f. Payment will be made in accordance with, and within the time specified, in Government Code Chapter 4.5 commencing with Section 927.

2. 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.

3. 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.

4. 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.

EXHIBIT C: COST WORKSHEET DETAILS

Company Name: Crayon Software Experts LLC

Offerors must submit a cost quote for each item(s) listed in the attached RFO Cost Worksheet and clearly state unit and extended cost as well as include subtotals and grand totals. Offeror must adhere to:

- Pricing is guaranteed from Software Assurance (SA) for all new enrollments of M365 GCC E5
- All future new enrollments shall qualify for "From SA" pricing
- During year 1 of this Agreement, all additional M365 GCC E5 licensing shall qualify for "From SA" pricing upon year 1 reconciliation
- Incremental additional M365 GCC E5 licenses added to enrollments for participating Customer Affiliates after year 1 anniversary shall be priced at "Full USL" pricing
- Pricing shall not exceed the negotiated discounts per applicable tier
- Pricing for all Microsoft products offered under this MELA shall be price protected throughout the term
- For products ordered at signing, the January 2021 price list will be the basis to determine final pricing
- Ensure applicable credits are applied to Year 1 and Year 2 (If applicable) cost based on customer's existing agreements prior to invoicing CDT
- Awarded Contractor may not mark up or mark down the credited amount to be applied to the Enrollment. The credit amount will be verified prior to award.
- All unit pricing on the Cost Worksheet must be to two decimal points only.
- Any unit pricing that exceeds two decimal points will be rounded down to the nearest cent.

In the event the new Enrollment starts with an initial commitment of M365 GCC E5 users that is below 200,000 users then the ramped pricing applicable to that tier will apply to all users for the term of the Enrollment or until the number of users reaches a total of 200,000. The discount ramp will also apply to the M365 GCC E5 components in the future pricing table and apply to all incremental users added to the Enrollment. The first order that brings the total number of users to 200,000 will receive the second tier of discounts and for all entities who started in the first discount tier, the future pricing table for M365 GCC E5 components will be re-set to the higher tier discount ramp upon anniversary, and the higher tier discount will apply to all incremental orders placed on the Enrollment.

Discount Tier 1 115,000 – 199,999 users	Discount Tier 2 200,000 users or more

All responses must include a copy of current level D rates. These rates shall apply for the term of this Agreement. If the number of total users falls below the 115,000 threshold, pricing shall revert to level D rates.

Microsoft PowerApps Promotional Offer

SKU	Item Name
SES-00001	PowerAppsperAppPlanGCCShrdSvr ALNG SubsVL MVL
SEL-00001	PowerAppsPlanGCCShrdSvr ALNG SubsVL MVLPerUsr

- 66% Discount applies only to net new PowerApps licenses in year one (1) of EA
- To maintain the discount into subsequent periods, the aggregate quantity of PowerApps licenses must be at least 30,000 30 days prior to Enrollment anniversary
- The discount will remain for each period the aggregate total is 30,000 or greater
- If the total quantity falls below 30,000, pricing will revert to Level D on the next anniversary

MELA/SCA Agreement #:	SCA-19-70-0204C
SB/DVBE Certification Number:	N/A
Retailers' Sellers Permit Number:	102-885166
FEIN Number:	47-2237420
Signature and Date:	2/17/2021
Printed Name and Title:	Ken Pharr, CFO
Company Name:	Crayon Software Experts LLC
Company Address:	12221 Merit Drive, Suite 800, Dallas, TX 75251
Contact Phone:	469-329-0290

EXHIBIT D: CALIFORNIA DEPARTMENT OF TECHNOLOGY

SPECIAL TERMS AND CONDITIONS TO SAFEGUARD FEDERAL TAX INFORMATION

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

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

I. PERFORMANCE

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

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

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

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

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

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

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

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

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

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such

person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

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

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.[1]

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

III. INSPECTION

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

REFERENCES

26 U.S.C. §6103(N)

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

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

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

(1) Equipment or other property, or

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

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

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

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

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

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

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

(2) That further inspection of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as 1 year, or both, together with costs of prosecution;

(3) That further disclosure of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as 5 years, or both, together with the costs of prosecution;

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

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

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

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

(2) Suspension of further disclosures of returns or return information by the

Service to the State tax agency, or to the Department of Justice, until the Service determines that such conditions and requirements have been or will be satisfied.

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

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

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

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

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

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

5.5.1 Agency Owned and Operated Facility

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

5.5.2 Contractor or Agency Shared Facility – Consolidated Data Centers

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

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

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

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

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

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

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

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

review and support required to resolve identified findings.

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

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

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

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

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

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

26 U.S.C. §7213. UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) Returns and return information

(1) Federal employees and other persons

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

(2) State and other employees

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

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

(3) Other persons

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

(4) Solicitation

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

(5) Shareholders

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

(b) Disclosure of operations of manufacturer or producer

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

(c) Disclosures by certain delegates of Secretary

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

(d) Disclosure of software

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

(e) Cross references

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

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

(2) Penalties for disclosure of confidential information

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

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

(a) Prohibitions

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

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

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

(2) State and other employees

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

(b) Penalty

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

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

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

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

(a) In general

(1) Inspection or disclosure by employee of United States

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

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

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

(b) Exceptions

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

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

(2) which is requested by the taxpayer.

(c) Damages

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

(1) the greater of -

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

(B) the sum of -

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

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

(2) the costs of the action, plus

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

(d) Period for bringing action

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

(e) Notification of unlawful inspection and disclosure

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

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

(2) section 7213A(a), or

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

(f) Definitions

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

(g) Extension to information obtained under section 3406

For purposes of this section -

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

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

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

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

EXHIBIT E: SECURITY AND DATA PROTECTION

Contractor shall certify to The National Institute of Standards and Technology (NIST) 800-171 standard and the DGS Cloud Computing Services Special Provisions publication requirements. At a minimum, provision shall cover the following:

1. The Contractor assumes responsibility of the confidentiality, integrity and availability of the data under its control. The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement to secure such data from data breach or loss, protect the data and information assets from breaches, introduction of viruses, disabling of devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its data or affects the integrity of that data.

2. Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A.

3. The Contractor shall comply with statewide policies and laws regarding the use and protection of information assets and data. Unauthorized use of data by Contractor or third parties is prohibited.

4. Signed Security and Confidentiality Statement for all personnel assigned during the term of the Agreement.

5. Apply security patches and upgrades, and keep virus protection software up-to-date on all information asset on which data may be stored, processed, or transmitted.

6. The Contractor shall notify the State data owner immediately if a security incident involving the information asset occurs.

7. The State data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation. The Contractor shall allow the State reasonable access to security logs, latency statistics, and other related security data that affects this Agreement and the State's data, at no cost to the State.

8. The Contractor shall be responsible for all costs incurred by the State due to security incident resulting from the Contractor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, destruction; loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the State. If the State data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.

9. The Contractor shall immediately notify and work cooperatively with the State data owner to respond timely and correctly to public records act requests.

10. The Contractor will dispose of records of State data as instructed by the State during the term of this agreement. No data shall be copied, modified, destroyed or deleted by the Contractor other than for normal operation or maintenance during the Agreement period without prior written notice to and written approval by the State.

11. Remote access to data from outside the territorial United States, including remote access to data by authorized support staff in identified support centers, is prohibited unless approved in advance by the State.

12. The physical location of Contractor's data center where the Data is stored shall be within the territorial United States.

EXHIBIT F: HIPAA Business Associate Agreement

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Data or FastTrack Data, execution of a license agreement that includes the Online Services Terms ("Agreement") will incorporate the terms of this HIPAA Business Associate Agreement ("BAA") into that Agreement. If there is any conflict between a provision in this BAA and a provision in the Agreement, this BAA will control.

1. Definitions.

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

"Breach Notification Rule" means the Breach Notification for Unsecured Protected Health Information Final Rule.

"Business Associate" shall have the same meaning as the term "business associate" in 45 CFR § 160.103 of HIPAA.

"Covered Entity" shall have the same meaning as the term "covered entity" in 45 CFR § 160.103 of HIPAA.

"Customer", for this BAA only, means Customer and its Affiliates.

"FastTrack Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by or on behalf of Customer for Microsoft's performance of the FastTrack Services.

"FastTrack Services" means the onboarding and migration services for Office 365 Services specified as being in scope for this BAA on the FastTrack Center BAA site at http://aka.ms/FastTrackBAA (or successor site) that are provided to Customer by Microsoft in connection with Customer's subscription for Office 365 Services, excluding services that are performed using third-party software or software that is not hosted by Microsoft.

"HIPAA" collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

"Microsoft Online Services", for this BAA only, means Office 365 Services, Microsoft Azure Core Services, Microsoft Dynamics 365 Core Services, Microsoft Intune Online Services, Microsoft Power Platform Core Services, and/or Microsoft Cloud App Security, each as defined in the "Data Protection Terms" section of the Online Services Terms incorporated into the Agreement; Microsoft Healthcare Bot; and any additional Azure online services and U.S. Government online services listed as in scope for this BAA on the Microsoft Trust Center at https://www.microsoft.com/en-us/trustcenter/Compliance/HIPAA (or successor site); excluding Previews.

"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information.

"Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by Microsoft from, or created, received, maintained, or transmitted by Microsoft on behalf of, Customer (a) through the use of the Microsoft Online Services or (b) for Microsoft's performance of the FastTrack Services.

"Security Rule" means the Security Standards for the Protection of Electronic Protected Health Information.

2. Permitted Uses and Disclosures of Protected Health Information.

a. **Performance of the Agreement for Microsoft Online Services.** Except as otherwise limited in this BAA, Microsoft may Use and Disclose Protected Health Information for, or on behalf of, Customer as specified in the Agreement; provided that any such Use or Disclosure would not violate HIPAA if done by Customer, unless expressly permitted under paragraph b of this Section.

b. **Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this BAA, Microsoft may Use and Disclose Protected Health Information for the proper management and administration of Microsoft and/or to carry out the legal responsibilities of Microsoft, provided that any Disclosure may occur only if: (1) Required by Law; or (2) Microsoft obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Microsoft of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Responsibilities of the Parties with Respect to Protected Health Information.

a. **Microsoft's Responsibilities.** To the extent Microsoft is acting as a Business Associate, Microsoft agrees to the following:

(i) **Limitations on Use and Disclosure.** Microsoft shall not Use and/or Disclose the Protected Health Information other than as permitted or required by the Agreement and/or this BAA or as otherwise Required by Law. Microsoft shall not disclose, capture, maintain, scan, index, transmit, share or Use Protected Health Information for any activity not authorized under the Agreement and/or this BAA. Neither Microsoft Online Services nor FastTrack Services shall use Protected Health Information for any advertising, Marketing or other commercial purpose of Microsoft or any third party. Microsoft shall not violate the HIPAA prohibition on the sale of Protected Health Information. Microsoft shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.

(ii) **Safeguards.** Microsoft shall: (1) use reasonable and appropriate safeguards to prevent inappropriate Use and Disclosure of Protected Health Information other than as provided for in this BAA; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

(iii) **Reporting.** Microsoft shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Microsoft becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer's Unsecured Protected Health Information that Microsoft may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than five (5) business days after Microsoft's determination of a Breach. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with Microsoft's and Customer's legal obligations.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Microsoft's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this BAA by any means Microsoft selects, including through e-mail. Microsoft's obligation to report under this Section is not and will not be construed as an acknowledgement by Microsoft of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

(iv) **Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Microsoft shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Microsoft to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Microsoft with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. Microsoft remains responsible for its Subcontractors' compliance with obligations in this BAA.

(v) **Disclosure to the Secretary**. Microsoft shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Customer to the Secretary of the Department of Health and Human Services for purposes of determining Customer's compliance with HIPAA, subject to attorney-client and other applicable legal privileges. Microsoft shall respond to any such request from the Secretary in accordance with the Section titled "Disclosure of Customer Data" in the Agreement.

(vi) **Access.** If Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall within fifteen (15) days make access to such Protected Health Information available to Customer in accordance with 45 CFR § 164.524 of the Privacy Rule.

(vii) **Amendment.** If Microsoft maintains Protected Health Information in a Designated Record Set for Customer, then Microsoft, at the request of Customer, shall within fifteen (15) days make available such Protected Health

Information to Customer for amendment and incorporate any reasonably requested amendment

in the Protected Health Information in accordance with 45 CFR § 164.526 of the Privacy Rule.

(viii) **Accounting of Disclosure.** Microsoft, at the request of Customer, shall within fifteen (15) days make available to Customer such information relating to Disclosures made by Microsoft as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

(viii) **Performance of a Covered Entity's Obligations.** To the extent Microsoft is to carry out a Covered Entity obligation under the Privacy Rule, Microsoft shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

b. **Customer Responsibilities.**

(i) **No Impermissible Requests.** Customer shall not request Microsoft to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

(ii) **Contact Information for Notices.** Customer hereby agrees that any reports, notification, or other notice by Microsoft pursuant to this BAA may be made electronically. Customer shall provide contact information as follows (or as Microsoft may specify from time to time): (1) the Azure Security Center for Microsoft Azure Core Services, (2) MSO-HIPAA@microsoft.com for other Azure or U.S. Government online services in scope for this BAA, and (3) the Message Center in the Admin Center for other Microsoft Online Services. Contact information (a) for Microsoft Azure Core Services must include the security contact information required on the Azure Security Center, (b) for other Azure or U.S. Government online services in scope for this BAA must include name of individual(s) to be contacted, title of individual(s) to be contacted, e-mail address of individual(s) to be contacted, name of Customer organization, and, if available, Customer's contract number, subscriber identification number, and Microsoft Online Direct Routing Domain (MODRD) (e.g. "contoso.onmicrosoft.com"), and (c) for other Microsoft Online Services must include information required for the Message Center Privacy reader role in the Admin Center. Customer shall ensure that such contact information remains up to date during the term of this BAA. Failure to submit and maintain as current the aforementioned contact information may delay Microsoft's ability to provide Breach notification under this BAA.

(iii) **Safeguards and Appropriate Use of Protected Health Information.** Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to:

1) Not include Protected Health Information in: (1) information Customer submits to technical support personnel through a technical support request or to community support forums; and (2) Customer's address book or directory information. In addition, Microsoft does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data or FastTrack Data once it is sent to or from Customer outside Microsoft

Online Services or FastTrack Services over the public Internet, or if Customer fails to

follow applicable instructions regarding physical media transported by a common carrier.

2) Implement privacy and security safeguards in the systems, applications, and software Customer controls, configures, and uploads into the Microsoft Online Services or uses in connection with the FastTrack Services.

4. Applicability of BAA.

This BAA is applicable to Microsoft Online Services and FastTrack Services. Microsoft may, from time to time, (a) include additional Microsoft online services on the Microsoft Trust Center and/or in the "Data Protection Terms" section of the Online Services Terms incorporated into the Agreement or additional FastTrack Services on the FastTrack Center BAA site, and (b) update the definition of Microsoft Online Services and FastTrack Services in this BAA accordingly, and such updated definitions will apply to Customer without additional action by Customer. It is Customer's obligation to not store or process in an online service, or provide to Microsoft for performance of a professional service, protected health information (as that term is defined in 45 CFR § 160.103 of HIPAA) until this BAA is effective as to the applicable service.

5. Term and Termination.

a. **Term.** This BAA shall continue in effect until the earlier of (1) termination by a Party for breach as set forth in Section 5b, below, or (2) expiration of Customer's Agreement.

b. **Termination for Breach.** Upon written notice, either Party immediately may terminate the Agreement and this BAA if the other Party is in material breach or default of any obligation in this BAA. Either party may provide the other a thirty (30) calendar day period to cure a material breach or default within such written notice.

c. **Return, Destruction, or Retention of Protected Health Information Upon Termination.** Upon expiration or termination of this BAA, Microsoft shall return or destroy all Protected Health Information in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement. If it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, then Microsoft shall extend the protections of this BAA, without limitation, to such Protected Health Information and limit any further Use or Disclosure of the Protected Health Information to those purposes that make the return or destruction infeasible for the duration of the retention of the Protected Health Information.

6. Miscellaneous.

a. **Interpretation.** The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state law. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA.

b. **BAAs; Waiver.** This BAA may not be modified or amended except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.

c. **No Third-Party Beneficiaries.** Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, **upon** any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

d. **Severability.** In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.

e. **No Agency Relationship.** It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and Microsoft under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render Microsoft an agent of Customer.

EXHIBIT G: STATE OF CALIFORINA TERMS AND CONDITIONS

Cloud Computing-Software as a Service (SaaS)

(Effective 6/7/2019)

Information Technology General Provisions

(Revised and Effective (9/5/2014)