SCO ID: 7600-20217001

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
2021-7001	

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

CONTRACTING AGENCY NAME

California Department of Tax and Fee Administration

CONTRACTOR NAME

California Electronic Recording Transaction (CERTNA)

2. The term of this Agreement is:

START DATE

July 01, 2021

THROUGH END DATE

June 30, 2024

3. The maximum amount of this Agreement is:

$0.00 (Zero Dollar 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	Scope of Work	3
	Exhibit B	Budget Detail	1
	Exhibit C*	General Terms and Conditions (GSPD 401 IT)	Online
+ -	Exhibit D	Special Terms and Conditions	2
+ -	Exhibit E	Cloud Computing Services Special Provisions	5
+ -	Exhibit F	Additional Provisions	3

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.)

California Electronic Recording Transaction (CERTNA)

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
1115 Truxtun Avenue, 3rd Floor	Bakersfield	CA	93301

PRINTED NAME OF PERSON SIGNING	TITLE
CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
2021-7001	

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME			
California Department of Tax and Fee Administration			
CONTRACTING AGENCY ADDRESS	CITY	STATE	ZIP
450 N Street	Sacramento	CA	95814
PRINTED NAME OF PERSON SIGNING	TITLE		
Nga Pham	Manager, Acquisitions Branch		
CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED		
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)		
	SCM Vol. 1 4.04 A.2		

EXHIBIT A

SCOPE OF WORK

1. Summary

The purpose of this Agreement is for the California Electronic Recording Transaction Network Authority, a California Joint Powers Authority (JPA), herein referred to as the CERTNA, to provide the California Department of Tax and Fee Administration, herein referred to as the CDTFA or State, with online transmittal and recordation of business tax lien information through CERTNA's Government to Government (G2G) Portal. The CDTFA and the CERTNA are collectively hereinafter referred to as the Parties.

2. Points of Contact

The Contract Managers during the term of this Agreement will be:

CA Dept. of Tax & Fee Administration		CERTNA	
Name:	Craig Sampson	Name:	Brett Zamora
Address:	450 N Street, MIC: 55 Sacramento, CA 95814	Address:	1115 Truxtun Ave. 3rd Floor Bakersfield CA 93301
Phone:	(916) 309-5654	Phone:	(925) 683-7043
E-mail:	Craig.Sampson@cdtfa.ca.gov	E-mail:	Brett.Zamora@certna.com

All Technical Inquiries should be directed to:

CA Dept. of Tax & Fee Administration		CERTNA	
Name:	Rajaram Bondu	Name:	Brett Zamora c/o Certna
Address:	450 N Street Sacramento, CA 95814	Address:	1115 Truxtun Ave. 3rd Floor Bakersfield CA 93301
Phone:	(916) 309-5597	Phone:	(925) 683-7043
Email:	Rajaram.Bondu@cdtfa.ca.gov	E-mail:	Brett.Zamora@certna.com

Direct all agreement inquiries to:

CA Dept. of Tax & Fee Administration		CERTNA	
Name:	Contracts Section	Name:	Brett Zamora
Address:	450 N Street, MIC: 24 Sacramento, CA 95814	Address:	1115 Truxtun Ave. 3rd Floor Bakersfield, CA 93301
Phone:	(916) 322-2107	Phone:	(925) 683-7043
Email:	acquisitionscoor@cdtfa.ca.gov	Email:	Brett.Zamora@certna.com

Direct all Audit Request inquiries to:

CA Dept. of Tax & Fee Administration		CERTNA	
Name:	Sara Sheikholislam	Name:	Brett Zamora
Address:	450 N Street, MIC: 54 Sacramento, CA 95814	Address:	1115 Truxtun Ave. 3rd Floor Bakersfield, CA 93301
Phone:	(916) 445-0360	Phone:	(925) 683-7043
E-mail:	Sara.Sheikholislam@cdtfa.ca.gov	E-mail:	Brett.Zamora@certna.com

EXHIBIT A

SCOPE OF WORK (CONTINUED)

Either Contract Manager may be changed without a formal amendment to this Agreement. The changing Party will notify the other Party with a ten (10) day prior, written notice, which will contain the new Contract Manager's name, mailing address, phone & fax numbers, and email address.

3. CERTNA Responsibilities

a. The CERTNA shall retrieve from CDTFA, via encrypted secure file transfer methods, the delivery of lien information, including digital electronic records that are lien instruments of real estate transactions and lien releases, and deliver it in encrypted form to the designated County Recorder's Office within two (2) business days of receipt.

b. The CERTNA shall receive via encrypted secure file transfer methods from the County Recorder Offices lien recordation confirmation data and to provide this data to CDTFA along with the recording documents no later than the following business day after receiving the documents from the counties.

c. The CERTNA shall place the following warning banner on the CERTNA G2G Portal for unauthorized users and notes to members:

> WARNING! YOU ARE ACCESSING THE CALIFORNIA ELECTRONIC RECORDING TRANSACTION NETWORK AUTHORITY (CERTNA) COMPUTER SYSTEM. BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

d. CERTNA Member Counties using the G2G Portal are encouraged to record liens and return them to CERTNA no later than 5:00 PM Pacific Time on the same business day the digital documents are received.

e. The CERTNA shall not charge the CDTFA for the electronic transmittal and recordation of liens through the CERTNA G2G Portal.

EXHIBIT A

SCOPE OF WORK (CONTINUED)

4. CDTFA Responsibilities

a. The CDTFA shall transmit to the CERTNA, via CERTNA provided encrypted secure file transfer methods, digital electronic records that are lien instruments of real estate transactions for delivery to and recordation with the designated County Recorder Office(s). The digital records will include new liens, lien extensions and lien releases. The CDTFA will provide data for CERTNA to pull after CDTFA notifies CERTNA.

b. The CDTFA shall not make any software or hardware modifications to the CERTNA G2G Portal without CERTNA's prior written notification of not less than 30 days prior to implementation. The CDTFA will also be given time to test prior to full implementation.

c. The CDTFA agrees to comply with any and all reasonable reporting requirements established by CERTNA.

d. The CDTFA shall provide full cooperation in any auditing or monitoring of CDTFA's use of G2G conducted by CERTNA.

e. The CDTFA agrees to provide full cooperation with CERTNA in the design, development, implementation, monitoring and evaluation of services provided under this Agreement.

f. The CDTFA agrees to make available all records pertaining to services provided under this Agreement to CERTNA representatives for examination and audit for a period of not less than one year.

5. Amendments

This Agreement may be amended to extend the term for up to one (1) additional year. If the CDTFA exercises this option, it will initiate an amendment to extend the term of the Agreement No alteration or variation of the terms of this Agreement shall be valid unless made in writing and signed by the Parties, and no oral understanding or agreement not incorporated herein, shall be binding on either party.

EXHIBIT B

BUDGET DETAIL

This is a zero-dollar non-budgetary Agreement.

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

1. EXCISE TAX: The State of California is exempt from Federal Excise Taxes, and no payment will be made for any personal property taxes levied on the Contractor or on any taxes levied on employee wages. The State shall only pay for any State or local sales or use taxes on the services rendered or equipment supplied to the State pursuant to this Agreement.

2. SETTLEMENT OF DISPUTES: In the event of a dispute, Contractor shall file a "Notice of Dispute" with the Chief, Business Management Bureau of the CDTFA in Sacramento within ten (10) days of discovery of the problem. Within ten (10) days of receipt of the Notice, the Chief, Business Management Bureau, or his/her designee, shall meet with the Contractor and Contract Manager for purposes of resolving the dispute. The decision of the Chief, Business Management Bureau shall be final.

3. POTENTIAL SUBCONTRACTORS: Nothing contained in this Agreement or otherwise shall create any contractual relation between the State and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor agrees to be as fully responsible to the State for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by the Contractor. The Contractor's obligation to pay its subcontractors is an independent obligation from the State's obligation to make payments to the Contractor. As a result, the State shall have no obligation to pay or to enforce the payment of any moneys to any subcontractor.

4. CONFIDENTIALITY OF DATA: All financial, statistical, personal, technical and other data and information relating to the State's operations, which is designated confidential by the State and made available to the Contractor in order to carry out this Agreement, or which becomes available to the Contractor in carrying out this Agreement, 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 in writing to the Contractor by the State. The Contractor shall not, however, be required to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession, is independently developed by the Contractor outside the scope of this Agreement, or is rightfully obtained from third parties.

5. RIGHT TO TERMINATE: This Agreement is subject to cancellation by the State (in whole or part) upon thirty (30) days written notice. The State may cancel this Agreement without the 30-day written notice if, in its opinion the State finds cause for immediate termination. The State shall also be relieved of any payments should the Contractor fail to perform the requirements of this Agreement at the time and in the manner herein provided. In the event of such termination the State may proceed with the work in any manner deemed proper by the State. All costs to the State shall be deducted from any sum due the Contractor under this Agreement and the balance, if any, shall be paid to the Contractor upon demand.

6. FORCE MAJEURE: Neither Party shall be liable to the other for any delay in or failure of performance, nor shall any such delay in or failure of performance constitute default, if such delay or failure is caused by “Force Majeure.” As used in this section, “Force Majeure” is defined as follows: Acts of war and acts of God such as earthquakes, floods, and other natural disasters such that performance is impossible.

7. COMPUTER SOFTWARE COPYRIGHT LAWS: Contractor certifies that it has appropriate systems and controls in place to ensure that state funds will not be used in performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

EXHIBIT E

STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Software as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR SOFTWARE AS A SERVICE (SaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND SHOULD BE ACCOMPANIED BY, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). SECURITY REQUIREMENTS DESIGNATED IN THIS DOCUMENT ARE ASSUMING A NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) LOW CLASSIFICATION, UNLESS OTHERWISE SET FORTH IN THE SOW. A HIGHER CLASSIFICATION MAY REQUIRE DIFFERENT SECURITY REQUIREMENTS. 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

a) "**Cloud Software as a Service (SaaS**)" - The capability provided to the consumer is to use applications made available by the provider running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

b) "**Cloud Platform as a Service (PaaS)**" - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

c) "**Cloud Infrastructure as a Service (IaaS)**" - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

d) "**Data**" - means any information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the SaaS pursuant to this Contract. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

e) "**Data Breach**" - means any access, destruction, loss, theft, use, modification or disclosure of Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.

f) "**Encryption**" - Conversion of plaintext to ciphertext through the use of a Federal Information Processing Standards (FIPS) validated cryptographic algorithm. [FIPS 140-2]

g) "**Recovery Point Objective (RPO)**" - means the point in time to which Data can be recovered and/or systems restored when service is restored after an interruption. The Recovery Point Objective is expressed as a length of time between the interruption and the most proximate backup of Data immediately preceding the interruption. The RPO is detailed in the SLA.

h) "**Recovery Time Objective (RTO)**" - means the period of time within which information technology services, systems, applications and functions must be recovered following an unplanned interruption. The RTO is detailed in the SLA.

Terms

2. SaaS AVAILABILITY: Unless otherwise stated in the Statement of Work,

a) The SaaS shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).

b) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the Statement of Work.
c) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions – Information Technology.
d) Contractor shall provide advance written notice to the State in the manner set forth in the Statement of Work of any major upgrades or changes that will affect the SaaS availability.

3. DATA AVAILABILITY: Unless otherwise stated in the Statement of Work,

a) The Data shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
b) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the Statement of Work if the State is unable to access the Data as a result of:
    1) Acts or omission of Contractor;
    2) Acts or omissions of third parties working on behalf of Contractor;
    3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Contractor's server, to the extent such attack would have been prevented by Contractor taking reasonable industry standard precautions;
    4) Power outages or other telecommunications or Internet failures, to the extent such outages were within Contractor's direct or express control.
c) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions – Information Technology.

4. SaaS and DATA SECURITY:

a) In addition to the Compliance with Statutes and Regulations provision set forth in the General Provisions – Information Technology, Contractor shall certify to the State:
    1) The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;
    2) Compliance with the following:
        i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
        ii. Current NIST special publications 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Third party audit results and Contractor's plan to correct any negative findings shall be made available to the State upon request ;
        iii. Undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit. Third party audit results and Contractor's plan to correct any negative findings and implementation progress reports shall be made available to the State upon request; and
        iv. Privacy provisions of the Federal Privacy Act of 1974;
    3) Compliance with industry standards and guidelines applicable to the SaaS services being provided. Relevant security provisions may include, but are not limited to: Health Insurance Portability and Accountability Act of 1996, IRS 1075, Health Information Technology for Economic and Clinical (HITECH) Act, Criminal Justice Information Services (CJIS) Security Policy, Social Security Administration (SSA) Electronic Information Exchange Security Requirements, and the Payment Card Industry (PCI) Data Security Standard (DSS) as well as their associated Cloud Computing Guidelines.
b) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Contract to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data.
c) Contractor shall allow the State reasonable access to SaaS security logs, latency statistics, and other related SaaS security data that affect this Contract and the State's Data, at no cost to the State.
d) Contractor assumes responsibility for the security and confidentiality of the Data under its control.
e) No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by the State.

f) Remote access to Data from outside the continental United States, including remote access to Data by authorized SaaS support staff in identified support centers, is prohibited unless approved in advance in writing by:
   1) the Agency Information Security Officer, with written notice to the State Chief Information Security Officer, or
   2) in the absence of an Agency Information Security Officer, the State Chief Information Security Officer.

5. ENCRYPTION: Confidential, sensitive or personal information shall be encrypted in accordance with California State Administrative Manual 5350.1 and California Statewide Information Management Manual 5305-A.

6. DATA LOCATION: Unless otherwise stated in the Statement of Work and approved in advance in writing by:
   1) the Agency Information Security Officer, with written notice to the State Chief Information Security Officer, or
   2) in the absence of an Agency Information Security Officer, the State Chief Information Security Officer,

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

7. RIGHTS TO DATA: The parties agree that as between them, all rights, including all intellectual property rights, in and to Data shall remain the exclusive property of the State, and Contractor has a limited, non-exclusive license to access and use the Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to the Data, including user tracking and exception Data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of Data by Contractor or third parties is prohibited. For the purposes of this requirement, the phrase "unauthorized use" means the data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized.

8. TRANSITION PERIOD:

a) Unless otherwise stated in the SOW, for ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the State in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment.
c) During the Transition Period, SaaS and Data access shall continue to be made available to the State without alteration.
d) Contractor agrees to compensate the State for damages or losses the State incurs as a result of Contractor's failure to comply with this section in accordance with the Limitation of Liability provision set forth in the General Provisions - Information Technology.
e) Unless otherwise stated in the SOW, the Contractor shall permanently destroy or render inaccessible any portion of the Data in Contractor's and/or subcontractor's possession or control following the expiration of all obligations in this section. Within thirty (30) days, Contractor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
f) The State at its option, may purchase additional transition services as agreed upon in the SOW.

9. DATA BREACH: Unless otherwise stated in the Statement of Work,

a) Upon discovery or reasonable belief of any Data Breach, Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency. Contractor shall provide such notification within forty-eight (48) hours after Contractor reasonably believes there has been such a Data Breach. Contractor's notification shall identify:
   1) The nature of the Data Breach;
   2) The Data accessed, used or disclosed;
   3) The person(s) who accessed, used, disclosed and/or received Data (if known);
   4) What Contractor has done or will do to quarantine and mitigate the Data Breach; and
   5) What corrective action Contractor has taken or will take to prevent future Data Breaches.
b) Contractor will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Contractor until the Data Breach has been effectively resolved to the State's satisfaction.
c) Contractor shall quarantine the Data Breach, ensure secure access to Data, and repair SaaS as needed in accordance with the SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
d) Notwithstanding anything to the contrary in the General Provisions - Information Technology, in performing services under this Contract, and to the extent authorized by the State in the Statement of Work, Contractor may be permitted

by the State to use systems, or may be granted access to the State systems, which store, transmit or process State owned, licensed or maintained computerized Data consisting of personal information, as defined by Civil Code Section 1798.29 (g). If the Contractor causes or knowingly experiences a breach of the security of such Data, Contractor shall immediately report any breach of security of such system to the State following discovery or notification of the breach in the security of such Data. The State's Chief Information Security Officer, or designee, shall determine whether notification to the individuals whose Data has been lost or breached is appropriate. If personal information of any resident of California was, or is reasonably believed to have been acquired by an unauthorized person as a result of a security breach of such system and Data that is not due to the fault of the State or any person or entity under the control of the State, Contractor shall bear any and all costs associated with the State's notification obligations and other obligations set forth in Civil Code Section 1798.29 (d) as well as the cost of credit monitoring, subject to the dollar limitation, if any, agreed to by the State and Contractor in the applicable Statement of Work. These costs may include, but are not limited to staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach of the security of such personal information.

e) Contractor shall conduct an investigation of the Data Breach and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement.

10. DISASTER RECOVERY/BUSINESS CONTINUITY: Unless otherwise stated in the Statement of Work,

a) In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency. Contractor shall provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contactor shall inform the State of:
    1) The scale and quantity of the Data loss;
    2) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
    3) What corrective action Contractor has taken or will take to prevent future Data loss.
    4) If Contractor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.
b) Contractor shall restore continuity of SaaS, restore Data in accordance with the RPO and RTO as set forth in the SLA, restore accessibility of Data, and repair SaaS as needed to meet the performance requirements stated in the SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
c) Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement.

11. EXAMINATION AND AUDIT: In addition to the Examination and Audit provision set forth in the General Provisions - Information Technology, unless otherwise stated in the Statement of Work:

a) Upon advance written request, Contractor agrees that the State or its designated representative shall have access to Contractor's SaaS, operational documentation, records and databases, including online inspections, that relate to the SaaS purchased by the State.
b) The online inspection shall allow the State, its authorized agents, or a mutually acceptable third party to test that controls are in place and working as intended. Tests may include, but not be limited to, the following:
    1) Operating system/network vulnerability scans,
    2) Web application vulnerability scans,
    3) Database application vulnerability scans, and
    4) Any other scans to be performed by the State or representatives on behalf of the State.
c) After any significant Data loss or Data Breach or as a result of any disaster or catastrophic failure, Contractor will at its expense have an independent, industry-recognized, State-approved third party perform an information security audit. The audit results shall be shared with the State within seven (7) days of Contractor's receipt of such results. Upon Contractor receiving the results of the audit, Contractor will provide the State with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

12. DISCOVERY: Contractor shall promptly notify the State upon receipt of any requests which in any way might reasonably require access to the Data of the State or the State's use of the SaaS. Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency, unless prohibited by law from providing such notification. Contractor shall provide such notification within forty-eight (48) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at Contractor regarding this Contract without first notifying the State unless prohibited by law from providing such notification. Contractor agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Contractor shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

EXHIBIT F

ADDITIONAL PROVISIONS

1. ADDITIONAL TERMS AND CONDITIONS: This Agreement sets forth the terms and conditions of CDTFA's use of the CERTNA's Government to Government (G2G) multi-county Electronic Recording Transaction Network Distribution and Return System Portal. The CERTNA G2G shall consist of CDTFA's release and transmittal of electronic lien information through the CERTNA G2G system and to the County Recorder Offices of any and all counties served by CERTNA.

   The counties formed CERTNA to develop, own, maintain and operate an electronic recording network for the purpose of standardizing the electronic recordation of documents. CERTNA is a public entity separate from the counties that are parties to the Joint Powers Agreement, and may jointly authorize any power common to its member counties. The CERTNA Board has authority to exercise such powers on behalf of CERTNA and its member counties per Government Code section 6500 et seq., known as the Joint Exercise of Powers Act; and as set forth in the CERTNA Joint Powers Agreement, Section 4, "Powers".

   The Parties anticipate that additional counties will participate in CERTNA as members or clients, and may be added to the CERTNA portal during the term of this Agreement. Counties also may withdraw as members of CERTNA, as set forth in section 11 of the CERTNA JPA. CERTNA will notify the CDTFA within 30 days of the addition or withdrawal of affiliated counties. The Parties agree that an amendment to this Agreement is not required for the addition or withdrawal of counties.

2. LEGAL AUTHORITY: The CDTFA is authorized to apply a perfected and enforceable state tax lien pursuant to sections 6757, 8996, 30322, and 38532, 40158, 41124.1, 43413, 45451, 46421, 50123, 55141, and 60445 of the Revenue and Taxation Code. The State tax liens may be electronically recorded with the counties pursuant to Government Code section 27279, which authorizes county recorders to accept digital images and certain digital documents for recordation.

3. CANCELLATION: Notwithstanding the State's General Provisions – Information Technology (GSPD-401IT) or the State's Cloud Computing Special Provisions, either CDTFA or CERTNA may terminate this Agreement with prior written notice to the other if any material representation, warranty, agreement, or obligation contained or referred to in this Agreement has been breached, provided the aggrieved Party has given the other Party notice of such material breach and there has been a failure to cure such material breach within 30 days after receipt of such notice. For purposes of this section, a material breach is a substantial failure of performance under the Agreement which is significant enough to relieve the aggrieved Party of a duty of further performance under the Agreement and provides the right to cancel the Agreement.

4. ENHANCEMENTS AND UPGRADES: The Parties acknowledge that the CDTFA may remit suggestions for enhancements or upgrades to the G2G software for CERTNA's consideration, but they fully accept and agree that CERTNA is the sole and final authority on the functionality, enhancements or upgrades of G2G software.

ADDITIONAL PROVISIONS (CONTINUED)

5. INDEMNIFICATION: Notwithstanding the State's General Provisions – Information Technology (GSPD-401IT) or the State's Cloud Computing Special Provisions, each Party agrees to mutually indemnify and hold harmless the other Party as specified herein:

   - The CDTFA shall indemnify and save harmless CERTNA (its officers, trustees, agents, employees, members and contractors) from all claims and losses in connection with the performance of this Agreement to the extent such claims and losses are caused by CDTFA's intentional, reckless, or negligent acts or omissions relating to this Agreement.

   - CERTNA shall indemnify and save harmless CDTFA (its officers, agents or employees) from all claims and losses in connection with the performance of this Agreement to the extent such claims and losses are caused by CERTNA's intentional, reckless, or negligent acts or omissions relating to this Agreement.

6. STATEMENT OF CONFIDENTIALITY: The California Department of Tax & Fee Administration has tax and fee payer returns and other confidential data in its custody. Unauthorized inspection or disclosure of confidential data is a misdemeanor (Revenue and Taxation Code sections 9255, 7056.5, 30455, Gov. Code section 15570.84).

7. DATA OWNERSHIP: The confidential tax and fee information being provided under this Agreement remains the property of the CDTFA. The receiving party shall have a non-exclusive right to use and process the disclosed information for the purposes stated in this Agreement. This right shall be revoked immediately upon termination of this Agreement. Disclosure of this data does not transfer ownership of information to the receiving party.

8. EMPLOYEE ACCESS TO INFORMATION: The CERTNA agrees that the information obtained will be kept in the strictest confidence and shall make information available to its own employees and Contractors only on a "need to know" basis. The "Need to know" standard is met by authorized employees who need information to perform their official duties in connection with the uses of the information authorized by this Agreement. The CERTNA recognizes its responsibilities to protect the confidentiality of CDTFA's information and other information as provided by law and ensures such information is disclosed only to those individuals and of such purpose, as authorized by the respective laws.

9. DISCLOSURE OF CONFIDENTIAL INFORMATION: Any unwarranted disclosure or use of CDTFA information or any willful unauthorized inspection of the CDTFA files is an act punishable as a misdemeanor. Inspection is defined to mean any examination of confidential information. The CERTNA, in recognizing the confidentiality of CDTFA information, agrees to take all appropriate precautions to protect the confidential information obtained pursuant to this Agreement from unauthorized disclosure. The CERTNA will conduct oversight of its users with access to the confidential information provided under this Agreement, and will promptly notify the CDTFA of any suspected violations of security or confidentiality by its users.

EXHIBIT F

ADDITIONAL PROVISIONS (CONTINUED)

10. INFORMATION SYSTEM SECURITY: Information security is the protection of information systems and information against unauthorized access, use modification or disclosure – ensuring confidentiality, integrity and availability of information systems and information. Where applicable the CERTNA will provide a level of security and information integrity equal to or exceeding industry best practices as defined in National Institute of Standards and Technology (NIST) Special Publication 800 Series, http://csrc.nist.gov/publications/PubsSPs.html and comply with all state and federal laws.

11. INCIDENT REPORTING: Parties shall follow notification and disclosure procedures as required by law and Exhibit E, section 9 (attached), in the event of any breach of data security. The California Information Practices Act, California Civil Code 1798, et al., protects individuals' right to privacy. Civil Code section 1798.82 sets forth the processes a person or business doing business in the State California are to follow in the event of a breach of encrypted and/or unencrypted personal data belonging to any resident of California. The CERTNA shall, upon discovery of or reasonable belief of a possible Data Breach as defined in Exhibit E, including improper inspection or disclosure of CDTFA information and security incidents by a CERTNA Employee or Contractor or any other person, timely notify the CDTFA Information Security Officer in the manner described in Exhibit E, section 9, to provide the information described therein, as well as the following: (a) date and time the incident was discovered, (b) any actions at and following the time of discovery that were taken prior to notifying CDTFA, (c) the IP address of the affected computer(s), (d) the assigned name(s) of the affected computer(s), € the operating system of the affected computer(s), and (f) the location of the affected computer(s).

12. DESTRUCTION OF RECORDS: All records received by CERTNA from CDTFA and any database created, copies made, or files attributed to the records received will be returned or destroyed upon completion of the business purpose it was obtained for. The records shall be destroyed in a manner to be deemed unusable or unreadable and to the extent that an individual record can no longer be reasonably ascertained. CERTNA shall retain a log of how and when records were destroyed or returned to CDTFA.

13. SAFEGUARD AUDITS: The CDTFA retains the right to conduct on site safeguard review audits of the CERTNA's use of CDTFA information and security controls established. The CERTNA will be provided a minimum of seven (7) days written notice of a safeguard review being conducted by the CDTFA staff.