

**MEMORANDUM OF UNDERSTANDING
BETWEEN THE DEPARTMENT OF CHILD SUPPORT SERVICES AND THE CALIFORNIA ELECTRONIC
RECORDING TRANSACTION NETWORK AUTHORITY KNOWN AS CERTNA
FOR THE USE OF THE CERTNA GOVERNMENT TO GOVERNMENT (G2G) PORTAL**

THIS MEMORANDUM OF UNDERSTANDING (“MOU” or “Agreement”), made and entered into on **August 30, 2021** is between the California Electronic Recording Transaction Network Authority (CERTNA), a Joint Powers Authority (JPA), and the Department of Child Support Services (DCSS), the submitting party (“Government Agency”), recording electronically through the CeRTNA G2G Portal, for the purpose of electronically recording lien documents with participating County Recorders or County Clerk/Recorders (CCR). The CeRTNA and Government Agency are collectively referred to as the “Parties.”

WHEREAS, the CERTNA has developed and implemented a Government to Government electronic recordation system pursuant to Government Code Section 27279(b), and has entered into contracts with various California governmental agencies to implement the system;

WHEREAS, the CERTNA G2G System permits governmental agencies to record electronically various documents with participating counties; and

WHEREAS, the Government Agency seeks to participate in the CERTNA G2G system; and

WHEREAS, additional county recorders may participate in the CERTNA as members, and be added to the CERTNA portal during the term of this MOU. Counties may withdraw as members of CERTNA, as set forth in section 11 of the CERTNA JPA. The Parties agree that an amendment to this Agreement is not required for addition or withdrawal of affiliated CCRs.

WHEREAS, the rights and responsibilities established by this MOU are intended to assure the continuing security and lawful operation of the CERTNA G2G System under Government Code Section 27279; and

WHEREAS, Government Agency has obtained approval through the CERTNA G2G to transmit documents electronically to CCR; and

WHEREAS, the CERTNA G2G allows recording of recordable documents through electronic receipt and transmission as substitution for conventional paper-based document recording; and

WHEREAS, the Parties desire to ensure that transactions using electronically recorded documents are legally valid and enforceable for the mutual benefit of the parties to those transactions; and

WHEREAS, the Parties desire to set forth the rights and responsibilities for the electronic submission of documents for recording through the CERTNA G2G; and

WHEREAS, Government Agency agrees to act in compliance with the specifications set forth in this MOU, including all Exhibits and Attachments;

NOW THEREFORE, the Parties, for and in consideration of the mutual promises and agreements herein continued, do agree to the following:

Term

This MOU shall become effective and commence as of the date written above and shall end five years from that date or when terminated in writing by either party in accordance with this Agreement.

A. Government Agency Acknowledgements and Responsibilities

1. Government Agency agrees to provide the CERTNA lien data and documents via CERTNA electronic transfer for the purposes of recordation with the CCRs. Refer to the Interface Design Document (IDD): *Send Real Property Lien Recording to CERTNA*, Attachment 1 (Main) and Attachment 2 (Record Layout).
2. Government Agency is wholly responsible for the submission of data and documents, and agrees to abide by the procedures set forth by the CERTNA.
3. Government Agency will provide full cooperation in resolving any system issues related to the auditing or monitoring of its use of G2G conducted by the CERTNA.
4. Government Agency agrees to comply with any and all reasonable reporting requirements established by the CERTNA.

5. Government Agency will not perform any authentication administration to the CERTNA authentication system.
6. Government agency is expressly prohibited from making any software/hardware modification to the G2G system without written consent of CERTNA.
7. CERTNA G2G recording permits preparation, signature and/or transmission of documents, in electronic format. The electronic documents shall be considered the “original” record of the transaction in substitution for, and with the same intended effect as paper documents. In the case that such documents bear a digital, electronic or facsimile signature, those signatures shall have the same effect as paper documents or records bearing handwritten signatures.
8. By use of digital, electronic or facsimile to sign documents, Government Agency is bound by those electronic signatures affixed to any documents and the electronic signatures shall have the same legal effect as if the signatures were manually affixed to a paper version of the document.
9. This MOU is not assignable by the Government Agency either in whole or part, without the written consent of the Parties.

B. CERTNA Responsibilities

1. CERTNA will electronically submit liens via a CERTNA transfer method to the appropriate County Recorder’s Office on behalf of the Government Agency.
2. CERTNA will notify the Government Agency within thirty (30) days when any County Recorder is added to the CERTNA Portal.
3. CERTNA will notify the Government Agency within thirty (30) days when any County Recorder is removed from the CERTNA Portal.
4. CERTNA will make available lien data and documents submitted by the Government Agency, via CSE, within one (1) business day of submission to the appropriate County Recorder’s Office.
5. CERTNA will make available to the Government Agency, via CSE, the recorded data and document within one (1) business day of recording. Refer to the Interface Design Document (IDD): *Receive Real Property Lien Recording from CERTNA*, Attachment 3 (Main) and Attachment 4 (Record Layout).
6. CERTNA will retain lien data and document submitted by the Government Agency for thirty (30) days before purging the lien data.

7. CERTNA has exclusive administrative access to the authentication system. Access to the G2G software will be governed by an authentication system approved and maintained by the CERTNA.
8. CERTNA retains ownership of the G2G software and is responsible for any modifications, upgrades, or enhancements. The CERTNA will provide the Government Agency access to the G2G on an as-is basis. The Government Agency may submit suggestions for enhancements to CERTNA.
9. CERTNA has sole authority on the functionality, enhancements, or upgrades of the G2G software.
10. CERTNA may terminate access to the G2G, or any part thereof, or may terminate access of any authorized submitter, or any authorized staff, at any time it deems it necessary to protect G2G, to protect the public interest, to protect the integrity of public records, or to protect homeowners or real property owners from financial harm. No cause or action or liability against CERTNA or any government agency will arise from any decision of CERTNA to terminate or deny access of any person or entity to G2G. CERTNA will notify the Government Agency thirty (30) days prior to making any changes to its G2G system, impacting the Government Agency.
11. Except for the access of confidential information in unencrypted form, CERTNA will have the absolute right to monitor the performance of the Government Agency in the delivery of services provided under this agreement. The Government Agency will give full cooperation in any auditing or monitoring conducted. The Government Agency will cooperate with CERTNA in the implementation, monitoring, and evaluation of the agreement and comply with any and all reporting requirements established by CERTNA. All records pertaining to services under this agreement will be available for examination and audit by CERTNA representatives for a period of not less than one (1) year from contract execution.
12. CERTNA shall conduct ongoing monitoring of the G2G Portal in an effort to protect the integrity of the transmission process.
13. CERTNA shall test and maintain the G2G Portal software and hardware.
14. CERTNA will work with the individual participating CCR and Government Agency if the G2G Portal experiences delays or power failures that interfere with the normal course of business until the problem has been remedied.
15. CERTNA will coordinate the G2G Portal administration, training, policy creation, access control, testing activities, and establishment of contracts required for Government Agency to submit to participating CCRs.
16. CERTNA will provide written notice to the Government Agency within 30 calendar days if there are any changes to the requirements or specifications.

17. CERTNA shall immediately notify Government Agency of any security incident, including but not limited to attempts at or actual unauthorized access which could compromise or otherwise adversely affect Government Agency's data systems.

C. Joint Responsibilities of the Parties

1. All Parties to this MOU agree to adhere to security and confidential provisions outlined in Exhibit E, Information Privacy and Security Requirements, along with Attachment 1 of Exhibit E, Data Security Standards, for the protection of any information exchanged between the Government Agency and the CERTNA. Any exceptions or exclusions will be reflected in Attachment 2 of Exhibit E, Information Security Provisions to Account for Exceptions and Exclusions.
2. Maintain such records as required by State and Federal law or regulation and as the Government Agency and the CERTNA may jointly agree.
3. Designate staff to have primary responsibility for program and technical liaison and coordination of activities under this agreement and meet, when necessary, to further define specific program procedures. Either party may change the designated contact person by notification to the other party in writing.
4. Protect all data, documentation or other information designated confidential by either the Government Agency or the CERTNA and made available to the other party in order to carry out this MOU from unauthorized use or disclosure through observance of the same or more effective procedural requirements as used by the agency providing the materials. The identification of all such confidential data and information, as well as the providing agency's procedural requirements for protection of such data and information from the unauthorized use and disclosure will be provided in writing to the receiving agency by the providing agency. It is understood that the unauthorized release or other use of confidential information is punishable as a misdemeanor. It is understood that both parties will comply with the safeguarding of information requirements provided in Welfare and Institutions Code Section 11478.1, Family Code Section 17212, and Title 22, CCR Section 111430.
5. Revisions and/or amendments made to this MOU will be made by mutual and written consent.
6. Either party may terminate this MOU for any reason by serving the other party with prior written notice of at least (30) business days.

IN WITNESS WHEREOF, the parties hereto have caused this MOU to be executed and attested to by their proper officers thereunto duly authorized and their official seals to be hereto affixed, as of the day and year first above written.

GOVERNMENT AGENCY

Department of Child Support Agency (DCSS)

Approved by: Lesley Bell

Title: Deputy Director, Operations Division

Signature: _____

Dated: _____

CeRTNA

Approved by: Richard Sherman

Title: Strategic Operations Director

Signature:  _____

Dated: 08/26/21

Attachment 1
Interface Design Document (IDD) Record Layout
SEND REAL PROPERTY LIEN RECORDING TO CERTNA

File Name: Send Real Property Lien Recording Request to CERTNA

File ID: CERTNA_SEND_XXX_XXXXXXXXXX_yyyyMMdd.xml

XXX = FIPS Code
XXXXXXXXXX = Lien ID
yyyy = Year
MM = Month
dd = Day

Element Name	Attribute Name	Data Type	Data Format	Required	LOV?	Description	List of Values
REQUEST GROUP	PRIAVersionIdentifier	alpha-numeric		no	no	This field identifies the version number	
REQUESTING PARTY	_Name	alpha-numeric		yes	yes	This field identifies that the response file is for DCSS	DCSS
REQUESTING PARTY	_StreetAddress	alpha-numeric		yes	yes	This field identifies the street address of DCSS	PO Box 419064
REQUESTING PARTY	_StreetAddress2	alpha-numeric		no	no	This field identifies the street address of DCSS	
REQUESTING PARTY	_City	alpha-numeric		yes	yes	This field identifies the city of DCSS	Rancho Cordova
REQUESTING PARTY	_State	alpha-numeric		yes	yes	This field identifies the state of DCSS	CA
REQUESTING PARTY	_PostalCode	integer		yes	yes	This field identifies the postal code of DCSS	95741-9064
REQUESTING PARTY	_Identifier	integer		yes	yes	This field identifies the file as either Production or Test	Prod ID = 9707 Test ID = 9708

SUBMITTING PARTY	LoginAccountIdentifier	alpha-numeric		yes	yes	This Field identifies the Login Account Identifier for the Submitting Party	g2gsubmittinguser
SUBMITTING PARTY	_Name	alpha-numeric		yes	yes	This field identifies the Name of the Submitting Party	G2G Submitting Agent
REQUEST	RequestDateTime	date time	YYYY-MM-DDTHH:MM:SS	yes	no	This field contains the date and time of the file generation	
PRIA REQUEST	_RelatedDocumentsIndicator	alpha		yes	yes	This field identifies the file as Request Data	true
PACKAGE	CountyFIPSCode	integer		yes	yes	This field identifies the three digit county FIPS code that the Notice of Support Judgment is to be recorded with. The list of values provides the FIPS codes for all counties in California, but the value(s) provided in the file will reflect only those that are CeRTNA enabled.	001 ALAMEDA 003 ALPINE 005 AMADOR 007 BUTTE009 CALAVERAS 011 COLUSA 013 CONTRA COSTA 015 DEL NORTE 017 EL DORADO 019 FRESNO 021 GLENN 023 HUMBOLDT 025 IMPERIAL 027 INYO 029 KERN 031 KINGS 033 LAKE 035 LASSEN 037 LOS ANGELES 039 MADERA 041 MARIN 043 MARIPOSA 045 MENDOCINO 047 MERCED 049 MODOC 051 MONO 053 MONTEREY 055 NAPA 057 NEVADA

							059 ORANGE 061 PLACER 063 PLUMAS 065 RIVERSIDE 067 SACRAMENTO 069 SAN BENITO 071 SAN BERNARDINO 073 SAN DIEGO 075 SAN FRANCISCO 077 SAN JOAQUIN 079 SAN LUIS OBISPO 081 SAN MATEO 083 SANTA BARBARA 085 SANTA CLARA 087 SANTA CRUZ 089 SHASTA 091 SIERRA 093 SISKIYOU 095 SOLANO 097 SONOMA 099 STANISLAUS 101 SUTTER 103 TEHAMA 105 TRINIT 107 TULARE 109 TUOLUMNE 111 VENTURA 113 YOLO 115 YUBA
PACKAGE	StateFIPSCode	integer		yes	yes	This field captures the State FIPS Code "06" for California	06 CALIFORNIA
PACKAGE	SecurityType	alpha-numeric		yes	yes	This field identifies the Security Type	G
PACKAGE	Priority	alpha-numeric		yes	yes	This field identifies the priority	Standard
PRIA DOCUMENT	_Code	alpha-numeric		yes	yes	This field identifies the type of document in the request	NoticeOfSupportJudgment

PRIA DOCUMENT	DocumentSequenceIdentifier	integer		yes	yes	This field identifies the document number when it is contained in a series of documents. This should always be '1', as DCSS will always send one document per file.	1
PRIA DOCUMENT	_UniqueIdentifier	integer		yes	no	This field provides the unique identification number (Lien ID) generated by CSE and associated to the recording request when the lien request was generated in CSE.	
GRANTOR	_FirstName	alpha-numeric		no	no	This field contains the name of the Grantor, which is the name of the Non-Custodial Parent.	
GRANTOR	NonPersonEntityIndicator	alpha-numeric		no	yes	This field is required if the Grantor is provided. The valid value is false, and DCSS will always provide the value of false, as the Grantor will always be a person.	false
GRANTEE	_FirstName	alpha-numeric		no	no	This field contains the name of the Grantee derived as the Case Managing County's FIPS name that is	

						contained in the FIPS Table.	
GRANTEE	NonPersonEntityIndicator	alpha-numeric		no	yes	This field is required if the Grantee is provided. The valid value is true, and DCSS will always provide the value of true, as the Grantee will always be a non-person.	true
EMBEDDED FILE	_PagesCount	integer		yes	yes	This field contains the number of pages contained in the embedded TIFF image of the Notice of Support Judgment.	2
EMBEDDED FILE	Document	alpha-numeric		yes	no	This field contains embedded TIFF image of the recorded Notice of Support Judgment.	
RECORDING TRANSACTION IDENTIFIER	_Value	integer		yes	no	This field provides the unique identification number (Lien ID) generated by CSE and associated to the recording request when the lien request was generated in CSE.	

Attachment 2
Interface Design Document (IDD) Record Layout
RECEIVE REAL PROPERTY LIEN RECORDING FROM CERTNA

File Name: Receive Real Property Lien Information from CERTNA
File ID: {Priority}_{PrimaryRef}_yymmddhhmmssnnn.xml

{Priority} = Standard
{PrimaryRef} = Lien ID
yy = Year
mm = Month
dd = Day
hh = Hour
mm = Minute
ss = Second
nnn = Millisecond

Element Name	Attribute Name	Data Type	Data Format	Required	LOV?	Description	List of Values
REQUEST GROUP	PRIVersionIdentifier	alpha-numeric		no	no	This field identifies the version number	
REQUESTING PARTY	_Name	alpha-numeric		no	yes	This field identifies that the response file is for DCSS	DCSS
REQUESTING PARTY	_StreetAddress	alpha-numeric		no	yes	This field identifies the street address of DCSS	PO Box 419064
REQUESTING PARTY	_StreetAddress2	alpha-numeric		no	no	This field identifies the street address of DCSS	
REQUESTING PARTY	_City	alpha-numeric		no	yes	This field identifies the city of DCSS	Rancho Cordova

REQUESTING PARTY	_State	alpha-numeric		no	yes	This field identifies the state of DCSS	CA
REQUESTING PARTY	_PostalCode	integer		no	yes	This field identifies the postal code of DCSS	95741
REQUESTING PARTY	_Identifier	integer		yes	yes	This field identifies the file as either Production or Test	Prod ID = 9707 Test ID = 9708
SUBMITTING PARTY	LoginAccountIdentifier	alpha-numeric		no	yes	This Field identifies the Login Account Identifier for the Submitting Party	g2gsubmittinguser
SUBMITTING PARTY	_Name	alpha-numeric		no	yes	This field identifies the Name of the Submitting Party	G2G Submitting Agent
RESPONSE	RequestDateTime	date time	YYYY-MM-DDTHH:MM:SS	no	no	This field contains the date and time of the file generation	
RESPONSE_DATA - This is the child element of RESPONSE and the parent element for the following child elements							
PRIA REQUEST	_RelatedDocumentsIndicator	alpha		no	yes	This field identifies the file as Request Data	True

PACKAGE	CountyFIPSCode	integer	no	yes	<p>This field identifies the three digit county FIPS code that the Notice of Support Judgment has been recorded with.</p> <p>The list of values provides the FIPS codes for all counties in California, but the value(s) provided in the file will reflect only those that are CeRTNA enabled.</p>	001 ALAMEDA 003 ALPINE 005 AMADOR 007 BUTTE009 CALAVERAS 011 COLUSA 013 CONTRA COSTA 015 DEL NORTE 017 EL DORADO 019 FRESNO 021 GLENN 023 HUMBOLDT 025 IMPERIAL 027 INYO 029 KERN 031 KINGS 033 LAKE 035 LASSEN 037 LOS ANGELES 039 MADERA 041 MARIN 043 MARIPOSA 045 MENDOCINO 047 MERCED 049 MODOC 051 MONO 053 MONTEREY 055 NAPA 057 NEVADA 059 ORANGE 061 PLACER 063 PLUMAS 065 RIVERSIDE 067 SACRAMENTO 069 SAN BENITO 071 SAN BERNARDINO 073 SAN DIEGO 075 SAN FRANCISCO 077 SAN JOAQUIN
---------	----------------	---------	----	-----	--	--

							079 SAN LUIS OBISPO 081 SAN MATEO 083 SANTA BARBARA 085 SANTA CLARA 087 SANTA CRUZ 089 SHASTA 091 SIERRA 093 SISKIYOU 095 SOLANO 097 SONOMA 099 STANISLAUS 101 SUTTER 103 TEHAMA 105 TRINIT 107 TULARE 109 TUOLUMNE 111 VENTURA 113 YOLO 115 YUBA
PACKAGE	StateFIPSCode	integer		no	yes	This field captures the State FIPS Code "06" for California	06 CALIFORNIA
PACKAGE	SecurityType	alpha-numeric		no	yes	This field identifies the Security Type	G
PACKAGE	Priority	alpha-numeric		no	yes	This field identifies the priority	Standard
PRIA DOCUMENT	_Code	alpha-numeric		no	yes	This field identifies the type of document in the request	NoticeOfSupport Judgment
PRIA DOCUMENT	DocumentSequencelIdentifier	integer		no	yes	This field identifies the document number when	1

						it is contained in a series of documents. This should always be '1', as DCSS will always send one document per file.	
PRIA DOCUMENT	_UniquelIdentifier	integer		yes	no	This field provides the unique identification number (Lien ID) generated by CSE and associated to the recording request when the lien request was generated in CSE.	
GRANTOR	_FirstName	alpha-numeric		no	no	This field contains the name of the Grantor, which is the name of the Non-Custodial Parent.	

GRANTOR	NonPersonEntityIndicator	alpha-numeric		no	yes	This field is required if the Grantor is provided. The valid value is false, and DCSS will always provide the value of false, as the Grantor will always be a person.	false
GRANTEE	_FirstName	alpha-numeric		no	no	This field contains the name of the Grantee derived as the Case Managing County's FIPS name that is contained in the FIPS Table.	
GRANTEE	NonPersonEntityIndicator	alpha-numeric		no	yes	This field is required if the Grantee is provided. The valid value is true, and DCSS will always provide the value of true, as the Grantee will always be a non-person.	true

RECORDING ENDORSEMENT	_Identifier	integer		no	no	This field provides an identifier assigned by the County Recorders backend vendor.
RECORDING ENDORSEMENT	_OfficersName	alpha-numeric		no	no	This field identifies the name of the Recording Officer
RECORDING ENDORSEMENT	_InstrumentNumberIdentifier	alpha-numeric		yes	no	This field identifies the Instrument Number of the recorded Notice of Support Judgment
RECORDING ENDORSEMENT	_RecordedDateTime	date time	YYYY-MM-DDTHH:MM:SS	yes	no	This field identifies the date and time the Notice of Support Judgment was recorded

RECORDING FEE	RecordingEndorsementFeeAmount	alpha-numeric		no	no	This field is a child element of RECORDING ENDORSEMENT and _FEES. The field provides the fee amount. DCSS should ignore this value.	
RECORDING FEE	RecordingEndorsementFeeDescription	alpha-numeric		no	no	This field is a child element of RECORDING ENDORSEMENT and _FEES. The field provides the fee description. DCSS should ignore this value.	
EMBEDDED FILE	_PagesCount	integer		no	yes	This field contains the number of pages contained in the embedded TIFF image of the Notice of Support Judgment.	2

EMBEDDED FILE	Document	alpha-numeric		yes	no	This field contains embedded TIFF image of the recorded Notice of Support Judgment.	
STATUS	_Code	alpha-numeric		yes	yes	This field identifies the status of the returned document	Recorded
RECORDING TRANSACTION IDENTIFIER	_Value	integer		yes	no	This field provides the unique identification number (Lien ID) generated by CSE and associated to the recording request when the lien request was generated in CSE.	

Exhibit E Data Security Requirements

This Data Security Requirements Exhibit (hereinafter referred to as “this Exhibit”) sets forth the information privacy and security requirements Contractor is obligated to follow with respect to all DCSS data disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of DCSS pursuant to Contractor’s agreement with DCSS. DCSS and Contractor desire to protect the privacy and provide for the security of DCSS data pursuant to this Exhibit and in compliance with state and federal laws applicable to the DCSS data.

1. General Security Controls

- A. **Confidentiality Statement.** Contractor must sign a confidentiality statement prior to accessing DCSS data. The confidentiality statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies.
- B. **Security Awareness Training.** Contractor must complete security awareness training prior to accessing DCSS data and annually thereafter. Contractor must retain individual training records for four years.
- C. **Workstation/Laptop Encryption.** All workstations, laptops, devices (including smart phones) that process and/or store DCSS data must be encrypted, at a minimum, using Advanced Encryption Standard (AES), with a 128bit key or higher or successor standards. The encryption solution must be full disk encryption.
- D. **Server Security.** All servers containing DCSS data must be encrypted, at a minimum, using Advanced Encryption Standard (AES), with a 128bit key or higher or successor standards; and have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- E. **Minimum Necessary.** Only the minimum necessary amount of DCSS data required to perform necessary business functions may be copied, downloaded, or exported.
- F. **Removable Media Devices.** All electronic files that contain DCSS data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart devices tapes etc.). DCSS data must be encrypted, at a minimum, using Advanced Encryption Standard (AES), with a 128bit key or higher or successor standards.
- G. **Antivirus Software.** All workstations, laptops and other systems that process and/or store DCSS data must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- H. **Patch Management.** All workstations, laptops and other systems that process and/or store DCSS data must have operating system and application security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk

Exhibit E continued

assessment and vendor recommendations. At a minimum, emergency (vulnerability and active exploit) patches must be applied immediately, while critical patches must be applied within 30 days, moderate patches applied within 90 days and low patches within 120 days.

- I. **User IDs and Password Controls.** All users must be issued a unique username. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must not be stored in readable format on the computer. Password must be changed every 90 days for both privileged and non-privileged accounts. Password must be changed if revealed or compromised.
 1. Enforce a minimum password complexity of:
 - Fifteen characters
 - At least one numeric and at least one special character
 - A mixture of at least one uppercase and at least one lowercase letter
 2. Enforce password minimum lifetime restriction of one day
 3. Prohibit password reuse for 10 generations
 4. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
 5. Enforce password-protect system initialization (boot settings)
- J. **Data Sanitization.** All DCSS data must be sanitized using NIST Special Publication 800-88 or successor standard methods for data sanitization or successor standards when the DCSS data is no longer needed.
- K. **Unique Identification.** Contractor's network security architecture must be able to uniquely identify all access to DCSS data obtained and used in the performance of this Agreement.
- L. **Secure Areas.** Computer monitors, printers, hard copy printouts or any other forms of information accessed or obtained under the performance of this agreement must be placed so that they may not be viewed by the public or other unauthorized persons.
- M. **Investigation of Breaches and Security Incidents.** The Contractor shall immediately investigate any breach or security incident involving DCSS data. As soon as the information is known and subject to the legitimate needs of law enforcement, Contractor shall inform the DCSS Project Representative and the DCSS Chief Information Security Officer. DCSS shall have the right to participate in the investigation or conduct its own independent investigation and the Contractor shall cooperate fully in any such investigation. The Contractor shall be responsible for all costs incurred by DCSS due to any security incident arising from the Contractor's failure to perform, or negligent acts of Contractor or Contractor's personnel, when such failure to perform or negligent acts result in unauthorized disclosure, release, access, review, or destruction of DCSS data or loss, theft, and/or misuse of DCSS data. For purposes of this provision, Contractor's personnel include, but are not limited to, Contractor's officers, agents, employees, business partners, and subcontractors. If DCSS determines that notice to the individuals whose data has

Exhibit E continued

been disclosed, released, accessed, reviewed, destroyed, lost, stolen, and/or misused is appropriate, the Contractor will bear any and all costs associated with the notice or any mitigation selected by DCSS. Costs recoverable by DCSS against Contractor 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.

- N. **Public Records Act Cooperation.** Contractor acknowledges that all information exchanged between Contractor and DCSS pursuant to this Agreement is potentially subject to the California Public Records Act (CPRA) (Gov. Code, § 6250, et seq.) Such information in any format including, but not limited to: electronic, paper, email, text message, and data. Contractor shall immediately notify and work cooperatively with the DCSS to respond timely and correctly to any request made pursuant to the CPRA.

2. System Security Controls

- A. **System Timeout.** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 15 minutes of inactivity.
- B. **Warning Banners.** All systems containing DCSS data must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. Users must be directed to log off the system if they do not agree with these requirements.
- C. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DCSS data, or which alters DCSS data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. This logging must be included for all user privilege levels including, but not limited to, systems administrators. If DCSS data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- D. **Access Controls.** The system must use role-based access controls for all user authentications, enforcing the principle of least privilege.
- E. **Transmission Encryption.** All data transmissions of DCSS data outside the contractor's secure internal network must be encrypted using Advanced Encryption Standard (AES) or successor standards, with a 128bit key or higher. Encryption can be end-to-end at the network level, or the data files containing DCSS data can be encrypted. This requirement pertains to any type of DCSS data in motion such as website access, file transfer, and E-Mail.
- F. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting DCSS data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

Exhibit E continued**3. Audit Controls**

- A. **System Security Review.** All systems processing and/or storing DCSS data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing DCSS data must have a procedure in place to perform with sufficient regularity a review of system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing DCSS data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

4. Business Continuity / Disaster Recovery Controls

- A. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DCSS data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to securely backup DCSS data to maintain retrievable exact copies of DCSS data. The backups shall be encrypted. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore DCSS data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DCSS data.

5. Paper Document Controls

- A. **Supervision of Data.** DCSS data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DCSS data in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where DCSS data is contained shall be escorted and DCSS data shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** DCSS data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization or successor standards when the DCSS data is no longer needed.

Exhibit E continued

- D. **Removal of Data.** DCSS data must not be removed from the premises of the Contractor except with express written permission of DCSS.
- E. **Faxing.** Faxes containing DCSS data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.
- F. **Mailing.** DCSS data shall only be mailed using secure methods. Large volume mailings of DCSS data shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted using Advanced Encryption Standard (AES) or successor standards, with a 128bit key or higher.

Exhibit E continued

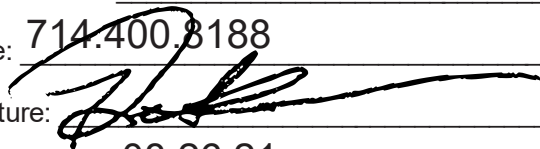
**CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES
CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT**

Information resources maintained by the California Department of Child Support Services and provided to Contractor may contain personal, confidential and/or sensitive information (PCSI) that is not open to the public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

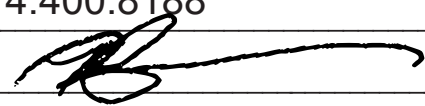
We hereby acknowledge that the PCSI of the DCSS is subject to strict confidentiality and security requirements imposed by state and federal law, which may include, but are not limited to the Information Practices Act – California Civil Code §1798 et seq., Public Records Act – California Government Code §6250 et seq., California Penal Code §502, 11140-11144, Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) – 45 CFR Parts 160 and 164, the California Welfare and Institutions Code §10850, Safeguarding Information for the Financial Assistance Programs – 45 CFR Part 205.50, Safeguarding and Disclosure of Confidential Information – 45 CFR Part 303.21, Title 26 United States Code sections 7213(a), 7213A, and 7431, California Family Code §17212, California Unemployment Insurance Code §1094, §2111 and §2122, and California Revenue and Taxation Code §7056 and §19542. Contractor agrees to comply with the laws applicable to the DCSS PCSI received.

The Confidentiality and Security Compliance Statement must be signed and returned with the Contract and must be signed and renewed on an annual basis.

Contractor Project Representative

Name (Printed): Richard Sherman
Title: Strategic Operations Director
Business Name: CeRTNA
Email Address: richard.sherman@certna.com
Phone: 714.400.8188
Signature: 
Date Signed: 08.26.21

Contractor Information Security Officer (or authorized official responsible for business' information security program)

Name (Printed): Richard Sherman
Title: Strategic Operations Director
Business Name: CeRTNA
Email Address: richard.sherman@certna.com
Phone: 714.400.8188
Signature: 
Date Signed: 08.26.21