Third Party Access (TPA)
Memorandum of Understanding

This Memorandum of Understanding, hereinafter referred to as MOU, also referred to by the Internal Revenue Service (IRS) as ("contract"), is between the California Department of Child Support Services hereinafter referred to as ("DCSS"), also referred to as ("Agency") by the IRS, 11150 International Drive, Rancho Cordova, CA 95670, and San Bernardino County Children and Family Services (hereinafter referred to as "Contractor"), also referred to as contractor by IRS), for the mutual administrative benefit of both parties. DCSS will provide to Contractor, on-line (IV-A or IV-E) read-only third-party access service to the Child Support Enforcement System ("CSE") as specified herein for the purpose of supporting the Child and Spousal Support Enforcement Program pursuant to Family Code 17212. The following terms and conditions apply to this MOU.

Contract Formation

1. The MOU is subject to any restrictions, limitations, or conditions enacted by the United States and the California State legislatures which may affect the provisions or terms herein in any manner.
2. This MOU, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of this MOU.
3. The following terms and conditions apply to this MOU, which is nonfinancial in nature with the limited exception of any potential costs identified below regarding communication connections and unauthorized disclosures.
4. The MOU may only be modified in writing, signed by both parties.
5. This MOU is effective on the date executed by the DCSS and shall be in effect for 36 months thereafter from the date of the Chief Information Security Officer's signature.
6. This MOU is subject to immediate termination by DCSS with cause.
7. Either party may terminate this MOU without cause upon thirty (30) days prior written notice of such termination. Termination initiated by Contractor must be directed to the DCSS contact described herein.
8. The MOU contacts and their respective contact information for this MOU are:

California Department of Child Support Services Information Security Office P. O. Box 419064 Rancho Cordova, CA 95741-9064 Info.security@dcss.ca.gov Phone: 916-464-5045	Responsible Party: Linda Miers Title: Supervising Office Assistant Agency Name: San Bernardino County Address: 860 E. Gilbert Street San Bernardino, CA 92415-0911 Email: lmiers@hss.sbcounty.gov Phone: 909-387-0481

Scope of DCSS Services

1. DCSS shall provide to Contractor with CSE (IV-A or IV-E) read-only online access as follows.

Requested Profile Access:
Profile Requested (IV-E or IV-A): IV-E
Purpose of Contractor Access:
i.e. Administration of welfare and foster care programs Administration of welfare and foster care programs

2. DCSS shall provide the Contractor online read-only IV-A or IV-E access.
3. DCSS shall provide Contractor's online access to CSE via the California Department of Technology (CDT) Data Center.

General Obligations of Contractor

1. Contractor shall allow audits or inspections by individuals authorized by DCSS at Contractor's premises during regular business hours, on three (3) business day's prior notice for purposes of determining compliance with the terms of this MOU. DCSS retains the right to examine records, security statements, system-generated logs, system storage media, network components and access terminals applicable to this MOU to determine compliance.
2. Contractor will implement and maintain the security of its system and components used for retrieval, transmittal, storage, and services used to access CSE as described in this MOU.
3. Contractor acknowledges all information in CSE is classified and must not be shared with unauthorized persons. Criminal and Civil Penalties may apply.
4. Contractor acknowledges that anyone who accesses CSE expressly consents to monitoring.
5. Contractor shall be responsible for the cost and maintenance of all communication connections between Contractor and CDT.
6. Contractor shall provide annually, by the last business day of January, the name, work address, phone, and email address of all CSE users in an excel format to DCSS.

Recusal

1. Contractor shall ensure that its employees never access or receive any case or participant information of any individual with whom they have a conflict. Below are examples of relationships that must be listed on the Recusal Form:

- The CSE user has an open or closed case.
- The CSE user has a relative with an open or closed case.
- The CSE user has a former spouse who has an open or closed case.
- The CSE user lives with a person who has an open or closed case.
- The CSE user has a former or current business acquaintance who has an open or closed case.

2. Contractor employees are required to recuse themselves from appropriate cases pursuant to this standard at the time of hire and at any time that the employee learns that there is a relationship, specified in this standard, with a child support participant in any case.
3. Contractor employees shall report any conflict of interest immediately to the DCSS.

Security Provisions

1. Contractor shall implement the following administrative safeguards. Contractor shall:
   a. Assign security and confidentiality responsibilities related to this MOU to its ISO and one (1) additional contact listed below. Contractor shall notify DCSS ISO in writing as soon as practical of any designee changes.

Name and Title	Contact Information (Address, Phone & Email)
Linda Miers	860 E. Gilbert Street San Bernardino, CA 92415-0911 909-387-0481 lmiers@hss.sbcounty.gov
Jennifer Lei Farris	825 E. Hospitality Lane, 2nd Floor San Bernardino, CA 92415 909-383-9750 Jennifer.Lei@hss.sbcounty.gov

   b. The TPA Entity point of contact/s who manages the user access and TPA Entity users must undergo and pass a background investigation prior to being permitted access to the CSE system, in accordance with the IRS Publication 1075 requirements. The background investigation includes a criminal history screening and citizenship/residency validation. Individuals must undergo reinvestigation at least every five (5) years.
   c. Implement policies and procedures to ensure that information obtained from CSE is used solely as provided for in this MOU and applicable laws, including, but not limited to, Family Code, section 17212.
   d. Make information available to its authorized personnel on a “need-to-know” basis and only for the purposes authorized under this MOU. “Need -to-know” refers to

those authorized persons who need information to perform their official duties in connection with the purpose described in this MOU.

e. Notify the DCSS Information Security Office (ISO) of any unauthorized disclosure involving information obtained from CSE as soon as practical, but no later than one (1) hour after an event is detected and cooperate with DCSS ISO in any investigation(s) of information security incidents. The notification must describe the incident in detail and provide contact information if different from the Information Security Officer described herein. In the event of a security incident, contact the ISO immediately at securityincidents@dcss.ca.gov or (916) 464-5045.

f. Contractor shall maintain a record of all authorized users, and level of access (IV-A or IV-E) granted to CSE information, based on job function. The record must include the first/last name, work address, telephone number and email address. The record must designate the last date the annual recusal form and annual confidentiality form were recorded, in addition to the last date the annual security training was completed. A copy of this record must be made available to DCSS upon request.

2. Contractor shall implement the following usage, duplication, and disclosure safeguards. Contractor shall:

   a. Use information only for purposes specifically authorized under the MOU and applicable federal and State laws. including, but not limited to: Title 26 United States Code sections 7213(a), 7213A, and 7431; California Penal Code section 502; California Family Code section 17212; California Unemployment Insurance Code sections 1094, 2111, and 2122; California Revenue and Taxation Code sections 7056, 7056.5, 19542, and 19542.1; and California Civil Code section, et seq. 1798.

   b. Protect CSE information against unauthorized access, at all times.

   c. Reproduce information in any form obtained under this MOU solely for purposes described herein.

   d. Refrain from publishing or selling information obtained under this MOU.

   e. Refrain from transmitting information obtained under this MOU without prior written approval from DCSS.

3. Contractor shall implement the following physical safeguards for CSE information. Contractor shall:

   a. Secure and maintain any computer systems, hardware, software, applications, and data that will be used in the performance of this MOU. This includes ensuring that all security patches, upgrades, and anti-virus updates are applied as appropriate to secure all information assets and date that may be used, transmitted or stored on such systems in the performance of this MOU.

   b. Safeguard equipment when used in public areas to access and view CSE information (e.g. during legal proceedings).

c. Restrict removal of CSE confidential information from Contractor's work location.

d. Store CSE information in a place physically secure from access by unauthorized persons.

4. Contractor shall implement the following management safeguards for CSE information. Contractor shall:

   a. Ensure that each user authorized to access CSE information completes the annual security awareness training issued by DCSS, pursuant to this MOU, and ensure that each user will only be provided access to CSE information on a need-to-know basis.
   b. Annually, obtain signed confidentiality statements and conflict recusal forms provided by DCSS ISO, from each user pursuant to this MOU.
      i. Retain confidentiality statements of each user for five (5) years.
   c. Maintain signed confidentiality statements and conflict recusal forms in an easily retrievable format and make statements available to DCSS ISO upon request.
   d. Ensure each user never access or receive any case or participant information of any individual with whom they have a conflict.
   e. Ensure each user recuse themselves from applicable cases pursuant to this standard at the time of hire and at any time that the user learns that there is a relationship, specified in this standard, with a child support participant in any case. Notify DCSS of any conflict case as they occur by submitting an updated conflict recusal form any time.

5. All changes to systems, storage media and network components used for CSE online access or services must be consistent and compatible with CSE technical configuration requirements. To ensure compatibility and compliance, the local ISO designated in this MOU must approve in writing all configurations prior to implementation. DCSS will monitor compliance with this requirement.

6. Contractor shall ensure that unique individual user identifiers and user-selected passwords for each person are utilized on every system capable of online CSE access.

7. Contractor shall ensure video terminals, printers, hard copy printouts or any other forms of CSE records are placed so that they may not be viewed by the public or other unauthorized persons. CSE information shall be destroyed when its business use has ended in a confidential manner such as incineration, mulching, pulping, disintegration, or shredding.

8. Contractor shall ensure terminals will not be left unattended while in active logon access session to CSE information unless secured by functioning locking device which prevents entry, viewing or receipt of information or secured in a locked room which is not accessible to unauthorized personnel. All devices which contain unique identification codes used by Contractor for verification of authorized access to CSE information shall be secured against tampering.

Performance

1. The CSE contains IRS data. 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 performed under the supervision of the contractor or the contractor's responsible employees.

   (2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available 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 this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is 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 and products will be given the same level of protection as required for the source material.

   (4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

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

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

CRIMINAL/CIVIL SANCTIONS

(1) 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 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 five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future 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 Internal Revenue Codes (IRC) 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to who 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 this 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 $1,000.00 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 $1,000.00 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. The penalties are prescribed by IRCs 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 DCSS 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 so prohibited, willfully discloses the material in any manner to any person or DCSS 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 DCSS'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 DCSS's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). 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. For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

INSPECTION

The IRS and the DCSS 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.

CONCLUSION

This Contract may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Contract. The parties shall be entitled to sign and transmit an electronic signature of this Contract (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Contract upon request.

Execution of Signatories

I have read and understand the MOU and agree to abide by the terms and conditions herein.

Contractor:
San Bernardino County

_____ Date _____
Print Name: Dawn Rowe
Chair, Board of Supervisors:
San Bernardino County

State of California
Department of Child Support Services

_____ Date:_____
Gulzar Jaggi
Chief Information Security Officer
Enterprise Architecture &
Security Branch