County of Los Angeles
Child Support Services Department

TERRIE HARDY
Director

DEAN DE GRUCCIO
Chief Deputy Director

December 03, 2024

ADOPTED
BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES
23 December 3, 2024

EDWARD YEN
EXECUTIVE OFFICER

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

RECOMMENDATION TO ACCEPT FEDERAL GRANT AWARD AND ENTER INTO A STATE CONTRACT FOR THE SECTION 1115 WAIVER PROJECT FOR EMPLOYMENT-LED SERVICES FOR NONCUSTODIAL PARENTS (3 VOTES) (ALL DISTRICTS)

SUBJECT

Request approval to enter into an intergovernmental agreement with the California Department of Child Support Services (CA DCSS) to enhance and expand the implementation of child support-led employment and other critical support services for under- and unemployed noncustodial parents residing in South Los Angeles (SOLA).

IT IS RECOMMENDED THAT THE BOARD:

1. Delegate authority to the Director of Child Support Services Department (CSSD) or her designee to execute CA DCSS Agreement Number 10-113 (Agreement) for $2,102,942 in US DHHS Office of Child Support Services grant funds to enhance child support-led employment and other critical support services for noncustodial parents throughout South Los Angeles (SOLA) effective from date of execution through September 29, 2029.
2. Delegate authority to the Director of CSSD or her designee to approve any required time extensions, modification, or amendments to the contract, and execute all required documents with the CA DCSS.
3. Delegate authority to the Director of CSSD or her designee to execute other documents, agreements, memoranda of understandings or contracts associated for the acceptance and use of this Agreement.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

In August 2024, the US DHHS Office of Child Support Services awarded CSSD with a five-year Section 1115 demonstration grant for CSSD's proposal, "SOLA Impact Outreach" project. The purpose of the project is to test whether offering under- and unemployed noncustodial parents with a broad range of employment and other critical services will result in increased child support payments, ultimately providing greater support for children.

Approval of the Agreement will provide additional resources to support a broad range of child support-led employment and other support services for noncustodial parents—breaking down silos by allowing federal child support funds to be used for employment, training, and critical support services such as fatherhood, mediation, financial literacy, substance abuse and others.

In partnership with the Departments of Economic Opportunity (DEO), Human Resources (DHR), Consumer and Business Affairs (DCBA), and other County departments, as well as several Community-Based Organizations (CBOs), the proposal would prioritize stakeholder engagement by creating a public-nonprofit network to provide a comprehensive array of services for up to 500 project noncustodial parent participants each year.

Examples of potential services offered to noncustodial parents in the demonstration project include:

o CSSD Enhanced Child Support Case Management teams offering services, such as debt reduction, suspension of enforcement tools, and expedited modification of child support orders;

o DEO offering employment, training, educational, workforce development, and other work support services, including dedicated Employment Specialists from America's Job Centers of California as well as partnering with DHR on training employment pathways into county employment.

o DHR offering training and employment programs tailored to noncustodial parents, including access to existing pipeline programs into Los Angeles County jobs. DHR will further explore development of a new pipeline program specifically targeted at noncustodial parents, contingent on needs assessments and stakeholder input.

o DCBA offering support services, such as mediation, financial education, referral to legal assistance and resources for immigrants, and other services to individuals through Counselors and in group settings like workshops; and,

o At least four CBOs with deep roots in SOLA communities offering critical mental health, substance use disorder, domestic violence, and Fatherhood programming services.

Implementation of Strategic Plan Goals

The recommended actions are consistent with the principles of the Countywide Strategic Plan, Goal 1: Make Investments That Transform Lives, by investing in solutions that address our most complex societal challenges (health, jobs, housing, food insecurity, and recidivism) affecting our most vulnerable communities – one person at a time.

FISCAL IMPACT/FINANCING

Requests for fiscal year activities will be submitted with the annual budget request. There will be no impact to the County General Fund.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

On February 2, 2024, the US DHHS Administration for Children and Families, Office of Child Support Services issued a Notice of Funding Opportunity inviting state and tribal Title IV-D child support agencies to apply for a Section 1115 waiver demonstration grant with an award ceiling of $2,102,942 over five years.
On March 19, 2024, on motion by Supervisor Holly J. Mitchell, the Board of Supervisors directed the Chief Executive Officer to submit a five-signature letter to the CSSD in support of the CSSD federal NextGen Demonstration grant proposal submitted on April 5, 2024.
August 29, 2024, CSSD received notice by the CA DCSS of their intention to award and intergovernmental agreement funded by US DHHS.
The terms and conditions of this Agreement are substantially similar to the terms and conditions of Attachment I and have been approved as to form by County Counsel (Attachment I).

CONTRACTING PROCESS

This project and Agreement will prioritize community engagement by creating a publicnonprofit network working together to provide a comprehensive array of services for up to 500 participants each year. CSSD plans to negotiate and execute up Memoranda of Understanding (MOUs) with CBOs.
CSSD will also partner with other County Departments to implement this project. MOUs will be executed with each department to memorialize the departmental roles and responsibilities.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of these actions will facilitate widespread implementation of child support-led employment services for noncustodial parents. It is anticipated that the results of this stakeholder-driven, interdepartmental and community-based project will demonstrate the benefits of systematically bridging the gap between child support and employment services at the Federal program level, and that ultimately, it may be expanded to support children and families throughout all five Supervisorial Districts.

CONCLUSION

Upon approval by the Board of Supervisors, it is requested that the Executive Officer/Clerk of the Board send an adopted stamped copy of the Board letter and attachments to CSSD.

Respectfully submitted,

TERRIE HARDY
Director

TH:GC

Enclosures

SCO ID: 5175-101113

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES
STANDARD AGREEMENT
STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
10-1113	

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

CONTRACTING AGENCY NAME
California Department of Child Support Services

CONTRACTOR NAME
Los Angeles County Child Support Services Department

2. The term of this Agreement is:

START DATE
November 27, 2024 or upon final signature or approval, whichever is later

THROUGH END DATE
September 29, 2029

3. The maximum amount of this Agreement is:
$2,102,942.00 - Two Million One Hundred Two Thousand Nine Hundred Forty-Two dollars 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	4
	Exhibit A.1	Project Summary and Goals	1
	Exhibit B	Budget Detail and Payment Provisions	2
+ -	Exhibit B.1	SOLA Impact Project Grant Budget	1
+ -	Exhibit C *	General Terms and Conditions - GTC	5
+ -	Exhibit D	Special Terms and Conditions	2
+ -	Exhibit E	Confidentiality and Information Privacy and Security Requirements	16
+ -	Exhibit E.1	Internal Revenue Service (IRS) Required Contract Language	4

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.)
Los Angeles County Department of Child Support Services

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
5770 S. Eastern Ave	Commerce	CA	90040

PRINTED NAME OF PERSON SIGNING	TITLE
Terrie Hardy	Director

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED

SCO ID: 5175-101113

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES
STANDARD AGREEMENT
STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
10-1113	

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME			
Department of Child Support Services			
CONTRACTING AGENCY ADDRESS	**CITY**	**STATE**	**ZIP**
P.O. Box 419064	Rancho Cordova	CA	95741
PRINTED NAME OF PERSON SIGNING	**TITLE**		
Nan Chen	Chief Financial Officer		
CONTRACTING AGENCY AUTHORIZED SIGNATURE	**DATE SIGNED**		
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	**EXEMPTION (If Applicable)**		
	SCM 1 4.06, B		

EXHIBIT A
SCOPE OF WORK

1. Project Purpose

   The Federal Office of Child Support Services (OCSS) has awarded the Next Generation Child Support Employment Services Demonstration Grant under a cooperative agreement to the California Department of Child Support Services (CA DCSS) for the purpose of establishing or enhancing child support-led employment and training programs for unemployed and underemployed noncustodial parents. This grant award is known federally and locally as the South Los Angeles (SOLA) Impact Project. Los Angeles County Child Support Services Department (CSSD) will seek to implement the project activities of the SOLA Impact Project.

   The proposed project design is outlined in Exhibit A.1, Project Summary and Goals. However, design details are guided by OCSS and the project evaluation team and remain fluid.

2. Project Period

   The term of this agreement is 5 years.

   Continuing project periods are dependent upon availability of federal funding and the renewal of non-competing continuation grant periods. CA DCSS may extend the agreement by executing an amendment after sending written notice of its intent to extend within 30 days of securing federal and state funding for continuing project periods.

3. Contract Managers

   The contract managers during the term of this Agreement will be:

Department of Child Support Services	Los Angeles Co. CSSD
Name: Emily Jernigan Address: P.O. Box 419064, Rancho Cordova, CA 95741-9064 Phone: 916-464-5259 Email: Emily.Jernigan@dcss.ca.gov	Name: Terrie Hardy, Director Address: 5770 S. Eastern Avenue, Commerce, CA 90040 Phone: 323-889-3400 Email: Terrie_Hardy@cssd.lacounty.gov

   Either party may change their contract manager upon providing 10 days written notice to the other party. Said changes shall not require an amendment to this Agreement.

4. Services to be Performed

A. For the duration of the contract period Los Angeles County CSSD will:

1) Designate one Project Manager - 1.0 Full Time Equivalent (FTE)

2) Designate one Data Coordinator - 0.24 FTE

3) Provide additional personnel costs in-kind.

4) Gather data analytics as requested for reporting requirements.

B. Los Angeles County CSSD Responsibilities:

The primary task of Los Angeles County CSSD is to ensure that the project is planned, implemented, and evaluated successfully at the site pursuant to the grant Funding Opportunity Announcement/OCSS Guidance. The Project Manager's tasks fall under two broad areas:

1) Project Development and Management:

a) Effectively maintain communication with project staff, including the Los Angeles County CSSD Director, Regional Administrator, CA DCSS Project Manager and partner agency staff.

b) Serve as primary local point of contact for CA DCSS, OCSS, and the Evaluation team.

c) Ensure successful collaboration with the CA DCSS, OCSS, Evaluation team, and partner agencies.

d) Serve as primary point of contact for Los Angeles County with the Evaluation team to ensure successful random assignment process and evaluation integrity.

2) Data Collection and Management:

a) Ensure timely notification of all evaluation-related data collection requests and determine whether sharing of such data is authorized.

b) Assist Los Angeles County CSSD and the Evaluation team, when necessary, with arrangements to obtain child support administrative data and administrative data of other agencies and programs, and materials that facilitate use of such data.

c) Ensure that all evaluation-related data collection and submission is appropriately staffed and managed with access to necessary technology,

and that program staff who will be responsible for collecting evaluation-related data receive necessary training from the Evaluation team.

d) Ensure CA DCSS is provided with all written documents that the Evaluation team distributes.

e) Review written documents the Evaluation team prepares/provides to your site and provide draft comments to CA DCSS in a timely manner, prior to submission.

f) Assist the Evaluation team in scheduling interviews, surveys, and any other required means of information collection for the purposes of program mapping and evaluation.

g) Assist the Evaluation team in scheduling any onsite visits conducted for training or data collection purposes.

h) Actively participate in Evaluation team onsite visits and work with Evaluation team to coordinate logistics and agenda, as requested, and arrange for participation by all key decision makers.

C. Reports:

Performance Progress Reports (PPR) are due semi-annually to OCSS and will be prepared by Los Angeles County CSSD. The draft PPRs will be submitted to CA DCSS for the Authorizing Official approval in a timely manner (no less than 15 days prior to the due date). CA DCSS will work with Los Angeles County CSSD to ensure all required reporting elements are appropriately documented for the identified reporting periods. The CA DCSS Project Manager will review and submit the final approved PPR's to OCSS via the GrantSolutions web portal.

Federal Financial Reports (FFR) are due semi-annually to OCSS. Los Angeles County CSSD will provide all financial information needed to complete the FFR as needed. CA DCSS Accounting will complete and submit the FFR as required to OCSS with input from Los Angeles County CSSD as needed.

D. CA DCSS Responsibilities:

CA DCSS has fiscal responsibility for the SOLA Impact Project. The CA DCSS Project Manager will dedicate six hours per month to program administration to assist with timely payment and compliant reporting.

The primary task of the Project Manager at CA DCSS is to ensure that the project is planned, implemented, and evaluated successfully pursuant to the grant Funding Opportunity Announcement/OCSS Guidance.

5. Third Party Agreements

   Third party agreements may be necessary during the course of the SOLA Impact Project. Any third-party agreements must clearly describe the project activities and support to which the third party is committing. All third-party agreements must detail the scope of work to be performed, work schedules, budget details, and other terms and conditions that structure or define the relationship. Agreements are subject to approval by the CA DCSS Authorizing Official, prior to execution. Third-party agreement must be signed by the person in the third-party organization with the authority to make such commitments on behalf of the organization. All final third-party agreements must be provided to CA DCSS, and upon request, to OCSS.

6. General Terms and Conditions

   Parties to this Agreement agree to comply with the requirements of the Department of Health and Human Services (HHS) Grants Policy Statement (HHS GPS), which can be found at https://www.acf.hhs.gov/policy-guidance/hhs-grants-policy-statement.

EXHIBIT A.1
PROJECT SUMMARY AND GOALS

Los Angeles County Child Support Services Department (CSSD) will establish or enhance child support-led employment and training programs for unemployed and underemployed noncustodial parents to help them gain employment and increase their earnings, which will increase the likelihood of receiving child support through income withholding. Providing employment and training services to unemployed noncustodial parents can improve the approach to child support service delivery by addressing a major reason for the nonpayment of child support, namely lack of employment and consistent income.

Los Angeles County CSSD will provide the following child support and related services to noncustodial parents who receive employment and training services:

- Initiating and expediting order review and, if appropriate, modification.
- Suspending certain enforcement tools as appropriate, such as removing license suspensions.
- Providing debt reduction as permitted by California state law.
- Assisting with obtaining custody and parenting time orders.

Project Goals:

The purpose of this project is to improve the financial well-being of children through reliable child support payments. The following project goals have been identified:

1. Deliver effective employment and training services in partnership with third-party employment service providers.

2. Increase the likelihood that noncustodial parents who receive employment and training services obtain employment and increase their earnings.

3. Increase child support collections through income withholding, providing a more reliable source of child support payments.

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. Invoicing and Payment

A. For services satisfactorily rendered, and upon receipt and approval of invoices, DCSS agrees to compensate Contractor for actual expenditures incurred in accordance with the rates, costs, or pricing specified in the Budget Detail.

B. The rates, costs, or pricing agreed upon in this Agreement will not increase for the term of this Agreement, including any amendments.

C. Itemized invoices will include the DCSS Agreement number and a detailed breakdown of rates, costs, or pricing per Budget Detail.

D. Invoices shall be submitted no more frequently than monthly in arrears via email to: DCSSVendorInvoices@dcss.ca.gov.

E. Final invoices for services must be received by DCSS within 90 days of the Agreement end date.

2. State Budget Contingency Clause

A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement, does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, DCSS shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

B. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, DCSS shall have the option to either cancel this Agreement with no liability occurring to DCSS or offer an Agreement amendment to Contractor to reflect the reduced amount.

3. Contracts with Federal Funds

A. It is mutually understood between the parties that this Agreement may have been written for the mutual benefit of both parties before ascertaining the availability of congressional appropriation of funds to avoid program and fiscal delays that would occur if the Agreement were executed after that determination was made.

B. This Agreement is valid and enforceable only if sufficient funds are made available to DCSS by the United States Government for the term of this Agreement for the purpose of this program. In addition, this Agreement is subject to any additional restrictions, limitations, or conditions enacted by Congress or to

any statute enacted by Congress that may affect the provisions, terms, or funding of this Agreement in any manner.

C. It is mutually agreed that if Congress does not appropriate sufficient funds for the program, this Agreement shall be amended to reflect any reduction in funds.

D. DCSS has the option to invalidate the Agreement under the 30-day cancellation clause or to amend the Agreement to reflect any reduction in funds.

4. Taxes

The State of California is exempt from federal excise taxes, and no payment will be made for any taxes levied on employees' wages. DCSS will pay for any applicable State of California or local sales or use taxes on the services rendered or equipment or parts supplied pursuant to this Agreement. DCSS may pay any applicable sales or use tax imposed by another state.

5. Travel

A. Any reimbursement for authorized travel and per diem shall be at rates not to exceed those amounts paid by the State in accordance with California Department of Human Resources (CalHR) rules and regulations.

1) In State - Mileage, per diem (meals and incidentals), and lodging rates: Travel Reimbursements - CalHR

2) Out of State: Human Resources Manual - CalHR

No travel outside the State of California shall be reimbursed unless prior written authorization is obtained from the State. [2 CCR 599.615 et seq.]

B. This is not to be construed as limiting Contractor from paying any differences in travel costs, from funds other than those provided by DCSS, between the CalHR rates and any rates Contractor is obligated to pay under other contractual agreements.

C. Contractor agrees to include these requirements in all contracts it enters into with subcontractors to provide services pursuant to this Agreement.

EXHIBIT B.1
SOLA IMPACT PROJECT GRANT BUDGET

Personel/Fringe Benefits	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Project Manager	108,000.00	108,000.00	74,000.00	74,000.00	74,000.00	438,000.00
Fringe Benefits	88,200.00	88,200.00	59,940.00	59,940.00	59,940.00	356,220.00
Data Coordinator	27,600.00	27,600.00	15,000.00	15,000.00	15,000.00	100,200.00
Fringe Benefits	22,400.00	22,400.00	12,150.00	12,150.00	12,150.00	81,250.00
Totals	246,200.00	246,200.00	161,090.00	161,090.00	161,090.00	**975,670.00**

Contractual	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Community-based Organizations	154,255.84	170,000.00	40,800.00	40,800.00	40,800.00	446,655.84
Other County Departments	108,000.00	95,000.00	61,200.00	61,200.00	61,200.00	386,600.00
Other	0.00	0.00	0.00	0.00	0.00	0.00
Totals	262,255.84	265,000.00	102,000.00	102,000.00	102,000.00	**833,255.84**

Travel (5 Travelers)	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Lodging	2,290.75	2,290.75	2,290.75	2,290.75	2,290.75	11,453.75
Meals	932.50	932.50	932.50	932.50	932.50	4,662.50
Allowance	980.00	980.00	980.00	980.00	980.00	4,900.00
Air Fare	2,000.00	2,000.00	2,000.00	2,000.00	2,000.00	10,000.00
Parking fees, other exps.	200.00	200.00	200.00	200.00	200.00	1,000.00
Totals	6,403.25	6,403.25	6,403.25	6,403.25	6,403.25	**32,016.25**

Equipment/Supplies/Construction	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Equipment	0.00	0.00	0.00	0.00	0.00	0.00
Supplies	4,900.00	3,000.00	3,000.00	3,000.00	3,000.00	16,900.00
Construction	0.00	0.00	0.00	0.00	0.00	0.00
Totals	4,900.00	3,000.00	3,000.00	3,000.00	3,000.00	**16,900.00**

Other	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Incentives	10,000.00	10,000.00	4,750.00	4,750.00	4,750.00	34,250.00
Emergency Needs	5,000.00	4,155.84	3,505.84	3,505.84	3,505.84	19,673.36
Totals	15,000.00	14,155.84	8,255.84	8,255.84	8,255.84	**0.00**

Indirect Costs	Year 1	Year 2	Year 3	Year 4	Year 5	Total
10% of Total Direct Costs	53,475.91	53,475.91	28,074.91	28,074.91	28,074.91	191,176.55
Totals	53,475.91	53,475.91	28,074.91	28,074.91	28,074.91	**191,176.55**

	Totals
Total Funds Year 1	588,235.00
Total Funds Year 2	588,235.00
Total Funds Year 3	308,824.00
Total Funds Year 4	308,824.00
Total Funds Year 5	308,824.00
Total Project Budget	2,102,942.00

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

1. Termination

Either party may terminate this Agreement for any reason upon 30 days prior written notice to the other party. This Agreement may be terminated immediately, to be followed by written notice, by either party upon material breach of the terms of this Agreement by the other party.

2. Audit of Federally Funded Agreements

A. Contractor agrees to comply with federal procedures in accordance with Title 45, Code of Federal Regulations (CFR) Part 75 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.

B. Both parties shall accept responsibility for receiving, replying to, and/or complying with any audit exceptions by appropriate federal audit agencies that are directly related to the services to be performed under this Agreement.

3. Amendments

DCSS reserves the right to amend this Agreement for additional time and to increase funding accordingly. No alteration or variation of the terms of this Agreement shall be valid unless made in writing and signed by the parties hereto.

Agreement amendments are subject to satisfactory performance and funding availability. Agreement amendments will not take effect until Contractor has received a copy of the final Agreement that has been signed by DCSS Procurement & Contracting Officer or designee.

4. Contract Language for General Services

Contractor agrees to comply with and assume responsibility for compliance by his/her employees of the terms and conditions of the Contract Language for General Services contained in Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities. The Contract Language for General Services, Exhibit 7, is found within the IRS Publication 1075 at the following website: http://www.irs.gov/pub/irs-pdf/p1075.pdf.

5. Dispute Resolution

In the event of a dispute, DCSS shall file a “Notice of Dispute” with the Chief Financial Officer of Contractor within 10 days of discovery of the problem. Within 10 days, the Chief Financial Officer or designee shall meet with the DCSS “Agency Designee” for purposes of resolving the dispute. The decision of the DCSS Chief Financial Officer shall be final.

6. Order of Precedence

In the event of any inconsistency between the terms, specifications, provisions, or attachments which constitute this Agreement, the following order of precedence shall apply:

A. Exhibit C, General Terms and Conditions for Interagency Agreements

B. STD 213, Standard Agreement

C. Exhibit A, Scope of Work

D. Any other attachments incorporated in the Agreement by reference.

EXHIBIT E
CONFIDENTIALITY AND INFORMATION PRIVACY AND SECURITY REQUIREMENTS

This Confidentiality and Information Privacy and 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 personal, confidential, and sensitive information (as defined herein) 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. (Such personal, confidential, and sensitive information is referred to herein as "DCSS PCSI".) DCSS and Contractor desire to protect the privacy and provide for the security of DCSS PCSI pursuant to this Exhibit and in compliance with state and federal laws applicable to the DCSS PCSI.

I. Order of Precedence: With respect to information privacy and security requirements for all DCSS PCSI, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the Agreement between Contractor and DCSS, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.

II. Effect On Lower Tier Transactions: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Contractor is obligated to follow with respect to DCSS PCSI 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. When applicable, Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of this Agreement between Contractor and DCSS, including this Exhibit, the following definitions shall apply:

A. Breach: "Breach" means, including but not limited to:

1. the unauthorized acquisition, access, use, or disclosure of DCSS PCSI in a manner which compromises the security, confidentiality, or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29, subdivision(f).

B. Confidential Information: "Confidential information" means that:

1. does not meet the definition of “public records” set forth in California Government Code section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of Section 7920.000, et seq. of the California Government Code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word “confidential” by DCSS.

C. Disclosure: “Disclosure” means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

D. PCSI: “PCSI” means “personal information,” “confidential information,” and “sensitive information” (as these terms are defined herein).

E. Personal Information: “Personal information” means information, in any medium (including but not limited to paper, electronic, oral) that:

1. directly or indirectly collectively identifies or uniquely describes an individual; or

2. could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

3. meets the definition of “personal information” set forth in California Civil Code section 1798.3, subdivision (a) or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5. meets the definition of “medical information” set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of “health insurance information” set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from disclosure under applicable state or federal law.

F. Security Incident: “Security Incident” means:

1. a suspected breach; or

2. the suspected or successful unauthorized access, disclosure, modification, or destruction of DCSS PCSI, in violation of any state or federal law or in a

manner not permitted under the agreement between Contractor and DCSS, including this Exhibit; or

3. the suspected or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability, or integrity of DCSS PCSI; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission involving DCSS PCSI. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

G. Federal Tax Information: "Federal Tax Information" means information in any medium (paper, electronic, oral) that:

1. consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including Internal Revenue Service (IRS) oversight;

2. is categorized as Sensitive But Unclassified information and may contain personally identifiable information;

3. includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration, Federal Office of Child Support Enforcement, Bureau of the Fiscal Service, or Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement; and

4. includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

H. Sensitive Information: "Sensitive Information" is information maintained by the DCSS, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information may be either public or confidential. Sensitive information is that information, for which disclosure would jeopardize the integrity of DCSS.

I. Use: “Use” means the sharing, employment, application, utilization, examination, or analysis of information.

IV. Disclosure Restrictions: Contractor and its employees, agents, and subcontractors shall protect from unauthorized disclosure any DCSS PCSI. Contractor shall not disclose, except as otherwise specifically permitted by the Agreement between Contractor and DCSS (including this Exhibit), any DCSS PCSI to anyone other than DCSS personnel or programs without prior written authorization from the DCSS Contract Manager/Administrator, except if disclosure is required by state or federal law.

V. Use Restrictions: Contractor and its employees, agents, and subcontractors shall not use any DCSS PCSI for any purpose other than performing Contractor's obligations under its Agreement with DCSS.

VI. Safeguards: Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of DCSS PCSI, including electronic or computerized DCSS PCSI. Contractor safeguards shall comply with guidelines and requirements contained in the IRS Publication 1075 at each location where DCSS PCSI exists under Contractor’s control. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of Contractor’s operations and the nature and scope of its activities in performing its Agreement with DCSS, including this Exhibit, and which incorporates the requirements of Section VII, Security, below. Upon request, Contractor shall provide or allow DCSS to view current and updated policies.

VII. Security: Contractor shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing DCSS PCSI. Policies, practices, and controls implemented by Contractor must meet the guidelines and requirements contained in the IRS Publication 1075. These steps shall include, at a minimum, complying with all the data system security precautions listed in the Contractor Data Security Standards set forth in Attachment 1 to this Exhibit.

VIII. Security Officer: At each place where DCSS PCSI is located, Contractor shall designate a Security Officer to oversee its compliance with this Exhibit and to communicate with DCSS on matters concerning this Exhibit.

IX. Training: Contractor and its employees, agents or subcontractors who are onboarded to work within DCSS network will receive security awareness training within DCSS; otherwise, Contractor shall provide, at a minimum, annual training on its obligations under this Exhibit, at its own expense, to all of its workforce members who assist in the performance of Contractor’s obligations under Contractor’s

Agreement with DCSS, including this Exhibit, or otherwise use or disclose DCSS PCSI. Workforce members shall not begin work or have access to DCSS information until they have completed this training.

A. Contractor shall require each workforce member who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

B. Contractor shall retain each workforce member's certifications for DCSS inspection for a period of five years following contract termination or completion.

C. Contractor shall provide DCSS with its workforce member's certifications within five business days of a request by DCSS for the workforce member's certifications.

X. Employee and Workforce Member Discipline: Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Contractor workforce members under Contractor's direct control who intentionally or negligently violate any provisions of this Exhibit.

XI. Breach and Security Incident Responsibilities:

A. Notification to DCSS of Breach or Security Incident: Contractor shall notify DCSS **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Exhibit), **and** within **24 hours by email or fax** of the discovery of any security incident (as defined in this Exhibit), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to DCSS immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the DCSS Contract Manager/Administrator and the DCSS Chief Information Security Officer, using the contact information listed in Section XI(F), below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves DCSS PCSI in electronic or computerized form, notification to DCSS shall be provided by calling the DCSS Information Security Office at the telephone numbers listed in Section XI(F), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Contractor as of the first day on which such breach or security incident is known to Contractor, or, by exercising reasonable diligence would have been known to Contractor. Contractor shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member of Contractor.

Contractor shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code section 1798.29. (California Civil Code 1798.29, subdivision (e), California Civil Code 1798.82, subdivision (f), and State Administrative Manual (SAM) section 5340, Incident Management.)

B. Investigation of Breach and Security Incidents: Contractor shall immediately investigate such breach or security incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Contractor shall inform the DCSS Contract Manager/Administrator and the DCSS Chief Information Security Officer of:

1. what data elements were involved, and the extent of the data disclosure or access involved in the breach, including, specifically, the number of individuals whose personal information was breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used the DCSS PCSI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the DCSS PCSI, or to whom it is known or reasonably believed to have had the DCSS PCSI improperly disclosed to them; and

3. a description of where the DCSS PCSI is believed to have been improperly used or disclosed; and

4. a description of the probable and proximate causes of the breach or security incident; and

5. whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: Contractor shall provide a written report of the investigation to the DCSS Contract Manager/Administrator and the DCSS Chief Information Security Officer as soon as practicable after the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence or further disclosure of data regarding such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether

Contractor is considered only a custodian and/or non-owner of the DCSS PCSI, Contractor shall, at its sole expense, and at the sole election of DCSS, either:

1. make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. Contractor shall inform the DCSS Chief Information Security Officer of the time, manner, and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2. cooperate with and assist DCSS in its notification (including substitute notification) to the individuals affected by the breach.

E. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, and regardless of whether Contractor is considered only a custodian and/or non-owner of the DCSS PCSI, Contractor shall, at its sole expense, and at the sole election of DCSS, either:

1. electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content and timeliness provisions of Section 1798.29, subdivision (e). Contractor shall inform the DCSS Chief Information Security Officer of the time, manner, and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2. cooperate with and assist DCSS in its submission of a sample copy of the notification to the Attorney General.

F. DCSS Contact Information: To direct communications to the above referenced DCSS staff, Contractor shall initiate contact as indicated herein. DCSS reserves the right to make changes to the contact information below by written notice to Contractor. Said changes shall not require an amendment to this Exhibit or the Agreement to which it is incorporated.

DCSS Contract Manager/Administrator	DCSS Chief Information Security Officer
Refer to the Scope of Work	Information Security Office California Department of Child Support Services P.O Box 419064, MS 410 Rancho Cordova, CA 95741-9064 Email: info.security@dcss.ca.gov Telephone: (916) 464-5045

XII. Documentation of Disclosures for Requests for Accounting: Contractor shall document and make available to DCSS or (at the direction of DCSS) to an individual such disclosures of DCSS PCSI, and information related to such disclosures, necessary to respond to a proper request by the subject individual for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

XIII. Requests for DCSS PCSI by Third Parties: Contractor and its employees, agents, or subcontractors shall promptly transmit to the DCSS Contract Manager/Administrator all requests for disclosure of any DCSS PCSI requested by third parties to the Agreement between Contractor and DCSS (except from an individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

XIV. Notification of Requests by Other Entities of DCSS PCSI: If Contractor and its employees, agents, or subcontractors receive a subpoena, warrant, other legal order, demand, or Public Records Act Request (collectively, a "Request"), seeking DCSS PCSI, it will promptly notify DCSS and provide a copy of the Request along with copies of Records or data in its possession that it believes are responsive to the Request. In the event of a Request, the parties agree to consult and cooperate with each other in their respective responses, as appropriate.

XV. Audits, Inspection, and Enforcement: DCSS may inspect the facilities, systems, books, and records of Contractor to monitor compliance with this Exhibit. Contractor will allow audits or inspections by individuals authorized by the DCSS ISO at Contractor premises during regular business hours, with 24-hour notice for purposes of determining compliance with the terms of this Agreement. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the DCSS Contract Manager/Administrator in writing.

XVI. Return or Destruction of DCSS PCSI on Expiration or Termination: Upon expiration or termination of the Agreement between Contractor and DCSS for any reason,

Contractor shall securely return or destroy the DCSS PCSI within 15 days of the expiration or termination of the Agreement. If return or destruction is not feasible, Contractor shall provide a written explanation within 15 days to the DCSS Contract Manager/Administrator and the DCSS Chief Information Security Officer, using the contact information listed in Section XI(F), above.

A. Retention Required by Law: If required by state or federal law, Contractor may retain, after expiration or termination, DCSS PCSI for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Contractor's obligations under this Exhibit shall continue until Contractor returns or destroys the DCSS PCSI or returns the DCSS PCSI to DCSS; provided however, that on expiration or termination of the Agreement between Contractor and DCSS, Contractor shall not further use or disclose the DCSS PCSI except as required by state or federal law.

C. Notification of Election to Destroy DCSS PCSI: If Contractor destroys the DCSS PCSI, Contractor shall certify in writing, to the DCSS Contract Manager/Administrator and the DCSS Chief Information Security Officer, using the contact information listed in Section XI(F), above, that the DCSS PCSI has been securely destroyed. The notice shall include the date and type of destruction method used.

XVII. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolve, and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new security standards as they become published and implement requirements imposed by regulations and other applicable laws relating to the security or privacy of DCSS PCSI.

XVIII. Assistance in Litigation or Administrative Proceedings: Contractor shall make itself and any subcontractors, workforce employees or agents assisting Contractor in the performance of its obligations under the Agreement between Contractor and DCSS, available to DCSS at no cost to DCSS to testify as witnesses, in the event of litigation or administrative proceedings being commenced against DCSS, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by Contractor, except where Contractor or its subcontractor, workforce employee or agent is a named adverse party.

XIX. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than DCSS or Contractor and their respective successors or assignees, any rights, remedies, obligations, or liabilities whatsoever.

XX. Interpretation: The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XXI. Survival: If Contractor does not return or destroy the DCSS PCSI upon the completion or termination of the Agreement, the respective rights and obligations of Contractor under Sections VI, VII and XII of this Exhibit shall survive the completion or termination of the Agreement between Contractor and DCSS.

ATTACHMENT 1
CONTRACTOR DATA SECURITY STANDARDS

1. General Security Controls

A. **Confidentiality Statement.** Contractor Project Representative and Information Security Officer must sign a confidentiality statement (Attachment 2 to this Exhibit). All persons that will be working with DCSS PCSI must sign a Confidentiality Statement (See example in Attachment 3 to this Exhibit). The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member **prior** to access to DCSS PCSI. The statement must be renewed annually. Contractor shall retain each person's confidentiality statement for DCSS inspection for a period of three years following contract termination.

B. **Workstation/Laptop Encryption.** All workstations, laptops, and devices (including smart phones) that process and/or store DCSS PCSI must be encrypted, at a minimum, using a FIPS 140-3 certified algorithm or successor standards, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk.

C. **Server Security.** All servers containing DCSS PCSI must be encrypted, at a minimum, using a FIPS 140-3 certified algorithm or successor standards, such as Advanced Encryption Standard (AES), with a 128bit key or higher; and have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

D. **Minimum Necessary.** Only the minimum necessary amount of DCSS PCSI required to perform necessary business functions may be copied, downloaded, or exported.

E. **Removable Media Devices.** All electronic files that contain DCSS PCSI 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.). PCSI must be encrypted, at a minimum, using a FIPS 140-3 certified algorithm or successor standards, such as Advanced Encryption Standard (AES), with a 128bit key or higher

F. **Antivirus Software.** All workstations, laptops, and other systems that process and/or store DCSS PCSI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

G. **Patch Management.** All workstations, laptops, and other systems that process and/or store DCSS PCSI 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 assessment and vendor recommendations. At a minimum, emergency (vulnerability and active exploit) patches must be applied immediately, while critical (vulnerability and no exploit known) patches must be applied within 30 days. At a maximum, all other applicable patches must be installed within 90 days of vendor release.

H. **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; must not be stored in readable format on the computer; must be changed every 60 days for privileged accounts or 90 days for non-privileged accounts; and 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 24 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).

I. **Data Sanitization.** All DCSS PCSI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the DCSS PCSI is no longer needed.

J. **Unique Identification**. Contractor's network security architecture must be able to uniquely identify all access to DCSS PCSI obtained and used in the performance of this Agreement.

K. **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 as described in the Agreement.

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 PCSI 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. User 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 PCSI, or which alters DCSS PCSI. 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 PCSI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence, seven years for systems storing or transmitting FTI.

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 PCSI outside Contractor's secure internal network must be encrypted using a FIPS 140-3 certified algorithm or successor standards, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end-to-end at the network level, or the data files containing DCSS PCSI can be encrypted. This requirement pertains to any type of DCSS PCSI in motion such as website access, file transfer, and email.

F. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting DCSS PCSI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

A. **System Security Review.** All systems processing and/or storing DCSS PCSI 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 PCSI must have a routine procedure in place to review system logs for unauthorized access.

C. **Change Control.** All systems processing and/or storing DCSS PCSI 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 PCSI 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 PCSI to maintain retrievable exact copies of DCSS PCSI. 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 PCSI 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 PCSI 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 PCSI 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 PCSI is contained shall be escorted and DCSS PCSI shall be kept out of sight while visitors are in the area.

C. **Confidential Destruction.** DCSS PCSI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization or successor standards when the DCSS PSCI is no longer needed.

D. **Removal of Data.** DCSS PCSI must not be removed from the premises of the Contractor except with express written permission of DCSS.

E. **Faxing.** Faxes containing DCSS PCSI 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 PCSI shall only be mailed using secure methods. Large volume mailings of DCSS PCSI shall be by a secure, bonded courier with a signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a DCSS approved solution.

ATTACHMENT 2
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 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 §7920.000 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.

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

Contractor Project Representative

Name (Printed): _____

Title: _____

Business Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____

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

Name (Printed): _____

Title: _____

Business Name: _____

Email Address: _____

Phone: _____

Signature: _____

Date Signed: _____

STATE OF CALIFORNIA - HEALTH AND HUMAN SERVICES AGENCY

CONFIDENTIALITY STATEMENT

DCSS 0593 (01/17/18)

ATTACHMENT 3

The Department of Child Support Services (DCSS) is responsible for securing Child Support information. DCSS takes this responsibility seriously. The information below describes serious consequences you are subject to in the event that you unlawfully access or disclose Child Support information. Child Support information includes data that is obtained from numerous organizations including, but not limited to: the Internal Revenue Service, the California Franchise Tax Board, the California Employment Development Department, and the California State Board of Equalization. This information is confidential. Child Support information also includes DCSS plans, processes, procedures, memoranda, correspondence, research documents, and statistical analysis concerning the DCSS Child Support Program. This information may be confidential. Confidential information in any form (e.g. paper, CDs, DVDs, computer drives, mobile computing devices, etc.) is not public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. DCSS strictly enforces information security. If you violate DCSS confidentiality policies, you may be subject to administrative, civil, and or criminal action.

You may only access confidential information if you have a specific Child Support business need for that information. You may only disclose confidential information to other individuals that have a specific Child Support business need for that information. If you access confidential information without a Child Support business need or if you disclose confidential information to another person that does not have a Child Support business need, you may be subject to discipline by your department, termination of your or your employer's contract, criminal fines, or imprisonment.

- Fines for confidentiality violations range from $1,000 to $20,000.
- Imprisonment for confidentiality violations ranges from 1 year to 5 years.
- In addition, you may be liable for damages to persons injured by your confidentiality violation.

By your signature and initials below, you acknowledge that confidential Child Support information is subject to strict confidentiality requirements imposed by state and federal law including, but not limited to: Title 26 United States Code sections 7213(a), 7213A, and 7431; Code of Federal Regulations, 45CFR303.21; 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.

READ AND INITIAL EACH OF THE STATEMENTS PRINTED BELOW

_____ I acknowledge that operating any computer providing access to Child Support information constitutes consent to monitoring of all system activity. Evidence of unauthorized use collected during monitoring may be used for adverse or criminal action. Logging on to any system providing access to Child Support information indicates acceptance of the DCSS Information Security Policy.

_____ I acknowledge responsibility for knowing the classification of Child Support information. If I do not know the classification of specific information, I will seek classification information from my supervisor.

_____ I acknowledge that wrongful access, use, modification, or disclosure of confidential information may be punishable as a crime and/or result in disciplinary and/or civil action taken against me.

_____ I acknowledge that wrongful access, inspection, use, or disclosure of confidential information for personal gain, curiosity, or any non-business-related reason is a crime under state and federal laws.

_____ I acknowledge that wrongful access, use, modification, or disclosure of confidential information is grounds for immediate termination of my organization's Child Support related contract.

_____ I hereby agree to protect Child Support information in any form, (e.g., paper, CDs, DVDs, computer drives, mobile computing devices, etc.) by:

- Accessing Child Support information only as needed to perform my Child Support business duties.
- Never accessing information for curiosity or personal reasons.
- Never showing confidential information to or discussion confidential information with anyone who does not have the need to know.
- Storing confidential information only in approved locations.
- Never removing sensitive or confidential information from the work site without authorization.

_____ I agree that I will not disclose my password(s) that provide me access to Child Support systems to any other person.

_____ I agree that I will not duplicate or download confidential Child Support information unless I am authorized to do so.

I certify that I have read and initialed the confidentiality statements printed above.

PRINT FULL NAME _____ SIGNATURE _____

PRINT EMPLOYER'S FULL NAME _____ DATE _____

EXHIBIT E.1
INTERNAL REVENUE SERVICE (IRS)
REQUIRED CONTRACT LANGUAGE

The source of this IRS required contract language is: IRS Publication 1075 "Tax Information Security Guidelines for Federal, State and Local Agencies and Entities" – Exhibit 7 (November 2021).

Note: For the purpose of this section, the "Contractor" is the state agency or entity receiving the Federal Tax Information and "agency" is the Department of Child Support Services. The IRS requires this contract language to be included in any contracts for processing, handling, storing, destructing, or transmitting Federal Tax Information.

I. PERFORMANCE

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

(1) All work will be performed under the supervision of the contractor.

(2) The Contractor and Contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format 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 or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The Contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

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

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

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and 202 obligated to the agency under this contract.

(12) For purposes of this contract, the term "Contractor" includes any officer or employee of the Contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI 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 FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1. (3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a Contractor access to FTI must be preceded by certifying that each officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A Contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency’s security policy and procedures provided before the initial certification and annually

thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements. 203

III. INSPECTION

The IRS and the agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.